



# Avira

Antivirus Suite

## User Manual

## Trademarks and Copyright

### Trademarks

Windows is a registered trademark of the Microsoft Corporation in the United States and other countries.  
All other brand and product names are trademarks or registered trademarks of their respective owners.  
Protected trademarks are not marked as such in this manual. This does not mean, however, that they may be used freely.

### Copyright information

Code provided by third party providers was used for Avira Antivirus Suite. We thank the copyright owners for making the code available to us.

For detailed information on copyright, please refer to "Third Party Licenses" in the program help of Avira Antivirus Suite.

### End User License Agreement - EULA

<https://www.avira.com/en/license-agreement>

### Privacy Policy

<https://www.avira.com/en/general-privacy>

# Table of Contents

<b>1. Introduction .....</b>	<b>7</b>
1.1 Icons and emphases .....	7
<b>2. Product information .....</b>	<b>9</b>
2.1 Delivery scope .....	9
2.2 System requirements .....	10
2.2.1 System requirements Avira Antivirus Suite.....	10
2.2.2 System requirements Avira SearchFree Toolbar.....	11
2.2.3 Administrator rights (since Windows Vista).....	12
2.3 Licensing and Upgrade .....	12
2.3.1 Licensing.....	12
2.3.2 Extending a license .....	13
2.3.3 Upgrading.....	13
2.3.4 License manager.....	13
<b>3. Installation and uninstallation .....</b>	<b>15</b>
3.1 Installation and uninstallation .....	15
3.2 Choosing an installation type .....	15
3.3 Pre-Setup .....	16
3.4 Performing an Express Installation .....	18
3.5 Performing a Custom Installation.....	18
3.6 Test product installation .....	19
3.7 Configuration Wizard.....	20
3.8 Changing an installation under Windows 7 .....	22
3.9 Choosing installation components .....	22
3.10 Uninstallation .....	24
<b>4. Overview of Avira Antivirus Suite.....</b>	<b>26</b>
4.1 User interface and operation .....	26
4.1.1 Control Center.....	26
4.1.2 Game Mode .....	29
4.1.3 Configuration .....	30

4.1.4	Tray icon .....	33
4.2	Avira SearchFree Toolbar .....	34
4.2.1	Use.....	35
4.2.2	Options .....	38
4.2.3	Uninstalling Avira SearchFree Toolbar under Windows 7.....	41
4.3	How to...? .....	42
4.3.1	Activate license .....	42
4.3.2	Activate product.....	43
4.3.3	Perform automatic updates .....	44
4.3.4	Start a manual update .....	45
4.3.5	Using a scan profile to scan for viruses and malware .....	46
4.3.6	Scan for viruses and malware using drag & drop .....	48
4.3.7	Scan for viruses and malware via the context menu .....	48
4.3.8	Automatically scan for viruses and malware .....	48
4.3.9	Targeted scan for Rootkits and active malware .....	50
4.3.10	React to detected viruses and malware.....	50
4.3.11	Handling quarantined files (*.qua).....	55
4.3.12	Restore the files in quarantine .....	57
4.3.13	Move suspicious files to quarantine .....	59
4.3.14	Amend or delete file type in a scan profile .....	59
4.3.15	Create desktop shortcut for scan profile .....	60
4.3.16	Filter events.....	60
4.3.17	Exclude email addresses from scan .....	61
5.	<b>System Scanner .....</b>	<b>62</b>
6.	<b>Updates.....</b>	<b>63</b>
7.	<b>FireWall.....</b>	<b>65</b>
8.	<b>FAQ, Tips.....</b>	<b>66</b>
8.1	Help in case of a problem.....	66
8.2	Shortcuts .....	70
8.2.1	In dialog boxes.....	70
8.2.2	In the help.....	71
8.2.3	In the Control Center.....	72
8.3	Windows Security Center .....	74
8.3.1	General.....	74
8.3.2	The Windows Security Center and your Avira product .....	75

8.4	Windows Action Center.....	77
8.4.1	General.....	77
8.4.2	The Windows Action Center and your Avira product.....	78
<b>9.</b>	<b>Viruses and more .....</b>	<b>83</b>
9.1	Threat categories.....	83
9.2	Viruses and other malware.....	86
<b>10.</b>	<b>Info and Service .....</b>	<b>91</b>
10.1	Contact address.....	91
10.2	Technical support.....	91
10.3	Suspicious files .....	92
10.4	Reporting false positives.....	92
10.5	Your feedback for more security .....	92
<b>11.</b>	<b>Reference: Configuration options.....</b>	<b>93</b>
11.1	System Scanner .....	93
11.1.1	Scan .....	93
11.1.2	Report.....	102
11.2	Real-Time Protection.....	103
11.2.1	Scan .....	103
11.2.2	Report.....	114
11.3	Update .....	115
11.3.1	Web server.....	115
11.4	FireWall.....	117
11.4.1	Windows Firewall .....	117
11.5	Web Protection .....	120
11.5.1	Scan .....	120
11.5.2	Report.....	128
11.6	Mail Protection .....	129
11.6.1	Scan .....	129
11.6.2	General.....	133
11.6.3	Report.....	134
11.7	Child Protection .....	135
11.7.1	Social Networks .....	136

11.8	Mobile Protection.....	137
11.9	General.....	137
11.9.1	Threat categories .....	137
11.9.2	Advanced protection.....	138
11.9.3	Password .....	141
11.9.4	Security.....	143
11.9.5	WMI .....	145
11.9.6	Events.....	146
11.9.7	Reports .....	146
11.9.8	Directories .....	146
11.9.9	Acoustic alerts.....	147
11.9.10	Alerts .....	148

# 1. Introduction

Your Avira product protects your computer against viruses, worms, Trojans, adware and spyware and other risks. In this manual these are referred to as viruses or malware (harmful software) and unwanted programs.

The manual describes the program installation and operation.

For further options and information, please visit our website:

<http://www.avira.com>

The Avira website lets you:

- access information on other Avira desktop programs
- download the latest Avira desktop programs
- download the latest product manuals in PDF format
- download free support and repair tools
- access our comprehensive knowledge database and FAQs for troubleshooting
- access country-specific support addresses.

Your Avira Team

## 1.1 Icons and emphases

The following icons are used:

Icon / designation	Explanation
✓	Placed before a condition which must be fulfilled prior to execution of an action.
►	Placed before an action step that you perform.
<b>Warning</b>	Placed before a warning when critical data loss might occur.
<b>Note</b>	Placed before a link to particularly important information or a tip which makes your Avira Antivirus Suite easier to use.

The following emphases are used:

Emphasis	Explanation
<i>Italics</i>	File name or path data.
	Displayed software interface elements (e.g. window section or error message).
<b>Bold</b>	Clickable software interface elements (e.g. menu item, navigation area, option box or button).



## 2. Product information

This chapter contains all information relevant to the purchase and use of your Avira product:

- see Chapter: [Delivery scope](#)
- see Chapter: [System requirements](#)
- see Chapter: [Licensing and Upgrade](#)
- see Chapter: [License Manager](#)

Avira products are comprehensive and flexible tools you can rely on to protect your computer from viruses, malware, unwanted programs and other dangers.

► Please note the following information:

### Warning

Loss of valuable data usually has dramatic consequences. Even the best virus protection program cannot provide one hundred percent protection from data loss. Make regular copies (Backups) of your data for security purposes.

### Note

A program can only provide reliable and effective protection from viruses, malware, unwanted programs and other dangers if it is up-to-date. Make sure your Avira product is up-to-date with automatic updates. Configure the program accordingly.

### 2.1 Delivery scope

Your Avira product has the following functions:

- Control Center for monitoring, managing and controlling the entire program
- Central configuration with user-friendly standard and advanced options and context-sensitive help
- System Scanner (on-demand scan) with profile-controlled and configurable scan for all known types of virus and malware
- Integration into the Windows User Account Control allows you to carry out tasks requiring administrator rights.
- Real-Time Protection (on-access scan) for continuous monitoring of all file access attempts

- ProActiv component for the permanent monitoring of program actions (for 32-bit systems only)
- Mail Protection (POP3 Scanner, IMAP Scanner and SMTP Scanner) for the permanent checking of emails for viruses and malware, including the checking of email attachments
- Avira SearchFree Toolbar, a search toolbar integrated in the web browser providing quick and convenient search options. It also includes widgets of the most common Internet functions.
- Web Protection for monitoring data and files transferred from the Internet using the HTTP protocol (monitoring of ports 80, 8080, 3128)
- Avira Social Network Protection, a monitoring tool, informs parents of their children's online activities. It checks their social network accounts for comments, photos etc. that may influence the child's reputation in a negative way or may indicate that the child is in danger.
- Avira Android Security app is not only focused on anti-theft measures. The app helps you to get back your mobile device once you have misplaced it, or even worse: if it has been stolen. Furthermore the app allows you to block incoming calls or SMS. Avira Android Security protects cell phones and smartphones running with the Android operating system.
- Integrated quarantine management to isolate and process suspicious files
- Rootkits protection for detecting hidden malware installed in your computer system (rootkits)  
(Not available under Windows XP 64 bit)
- Direct access to detailed information on the detected viruses and malware via the Internet
- Simple and quick updates to the program, virus definitions, and search engine through Single File Update and incremental VDF updates via a web server on the Internet
- User-friendly licensing in License Manager
- Integrated Scheduler for planning one-off or recurring jobs such as updates or scans
- Extremely high virus and malware detection via innovative scanning technology (scan engine) including heuristic scanning method
- Detection of all conventional archive types including detection of nested archives and smart extension detection
- High-performance multithreading function (simultaneous high-speed scanning of multiple files)

## 2.2 System requirements

### 2.2.1 System requirements Avira Antivirus Suite

Avira Antivirus Suite has the following requirements for successful use of the system:

**Operating system**

- Windows 8, newest SP (32 or 64 bit) or
- Windows 7, newest SP (32 or 64 bit) or
- Windows XP, newest SP (32 or 64 bit)

**Hardware**

- Computer with Pentium processor or later, at least 1 GHz
- At least 150 MB of free hard disk memory space (more if using quarantine for temporary storage)
- At least 1024 MB RAM under Windows 8, Windows 7
- At least 512 MB RAM under Windows XP

**Other requirements**

- For the program installation: Administrator rights
- For all installations: Windows Internet Explorer 6.0 or higher
- Internet connection where appropriate (see Preparing for installation)

### 2.2.2 System requirements Avira SearchFree Toolbar

The following requirements have to be met for a proper use of the Avira SearchFree Toolbar:

**Operating system**

- Windows 8, newest SP (32 or 64 bit) or
- Windows 7, newest SP (32 or 64 bit) or
- Windows XP, newest SP (32 or 64 bit)

**Web browser**

- Windows Internet Explorer 6.0 or higher
- Mozilla Firefox 3.0 or higher
- Google Chrome 18.0 or higher

**Note**

If necessary, please uninstall any previously installed search toolbars before you install the Avira SearchFree Toolbar. Otherwise you will not be able to install the Avira SearchFree Toolbar.


### 2.2.3 Administrator rights (since Windows Vista)

On Windows XP, many users work with administrator rights. However, this is not desirable from the point of view of security because it is then easy for viruses and unwanted programs to infiltrate computers.

For this reason, Microsoft introduced the "User Account Control" (UAC). The User Account Control is part of the following operating systems:

- Windows Vista
- Windows 7
- Windows 8

The User Account Control offers more protection for users who are logged in as administrators. Thus an administrator only has the privileges of a normal user at first. Actions for which administrator rights are required are clearly marked by the operating system with an information icon. In addition, the user must explicitly confirm the required action. Privileges will only then be increased and the administrative task will be performed by the operating system after this permission has been obtained.

The Avira Antivirus Suite requires administrator rights for some actions. These actions are marked with the following symbol: . If this symbol also appears on a button, administrator rights are required to carry out this action. If your current user account does not have administrator rights, the Windows dialog of the User Account Control asks you to enter the administrator password. If you do not have an administrator password, you cannot carry out this action.

## 2.3 Licensing and Upgrade

### 2.3.1 Licensing

In order to be able to use your Avira product, you require a license. You thereby accept the license terms.

The license is provided in the form of an activation code. The activation code is a code comprising letters and numbers that you will receive after purchasing the Avira product. The activation code contains the exact data of your license, i.e. which programs have been licensed for which period of time.

The activation code will be sent to you by email, if you have purchased your Avira product on the Internet or it is indicated on the product packaging.

In order to license your program, please enter your activation code to activate the program. The product activation may be performed during installation. However, you can also activate your Avira product after the installation in the License Manager, under **Help > License management**.

### 2.3.2 Extending a license

When your license is about to expire, Avira will send a slide-up reminding you to extend your license. To do so, you only have to click a link and you will be forwarded to the Avira online shop. However, it is also possible to extend the license of your Avira product through the License Manager, under **Help > License management**

If you have registered in the licensing portal of Avira, you can additionally extend your license directly online via the **License Overview** or select the automatic renewal of your license.

### 2.3.3 Upgrading

In the License Manager, you have the option of launching an upgrade for a product from the Avira desktop product family. Manual uninstallation of the old product and manual installation of the new product is not required. When upgrading from the License Manager, you enter the activation code for the product you want to upgrade into the License Manager input box. The new product is automatically installed.

To achieve high reliability and security for your computer, Avira sends a pop-up item to remind you to upgrade your system to the newest version. Just click the **Upgrade** link on the pop-up item and you will be guided to your product specific upgrade site.

You have the possibility to upgrade your current product, or you may obtain a more comprehensive product. The product overview page shows what kind of product you are using right now and offers the chance to compare your product to other Avira products. If you need more information click the **information** icon right beside the product name. If you want to remain on the same product, click **Upgrade** and the download of the new version starts immediately. If you would like to obtain a more comprehensive product, click the **Buy** button at the bottom of the product column. You will be automatically forwarded to the Avira online shop where you can do your purchase order.

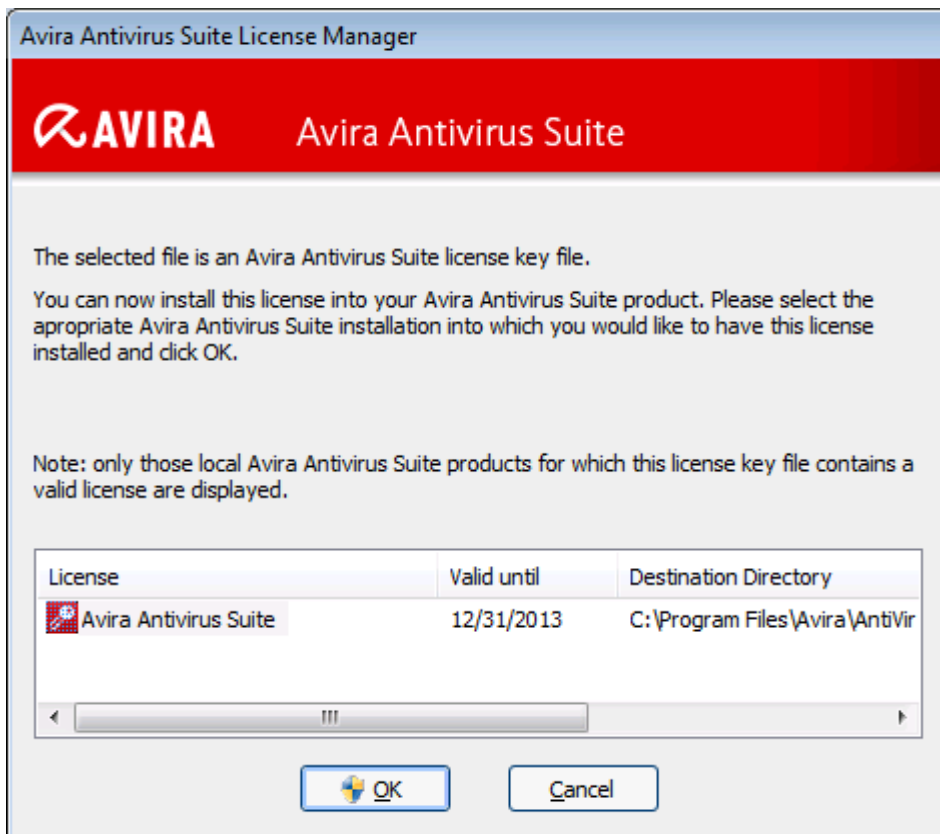
#### Note

Depending on your product and your operating system you may need administrator rights to perform the upgrade. Login as an administrator before performing an upgrade.

### 2.3.4 License manager

The Avira Antivirus Suite License Manager enables very simple installation of the Avira Antivirus Suite license.

## Avira Antivirus Suite License Manager



You can install the license by selecting the license file in your file manager or in the activation email with a double click and following the relevant instructions on the screen.

### Note

The Avira Antivirus Suite License Manager automatically copies the corresponding license in the relevant product folder. If a license already exists, a note appears as to whether the existing license file is to be replaced. In this case the existing file is overwritten by the new license file.

## 3. Installation and uninstallation

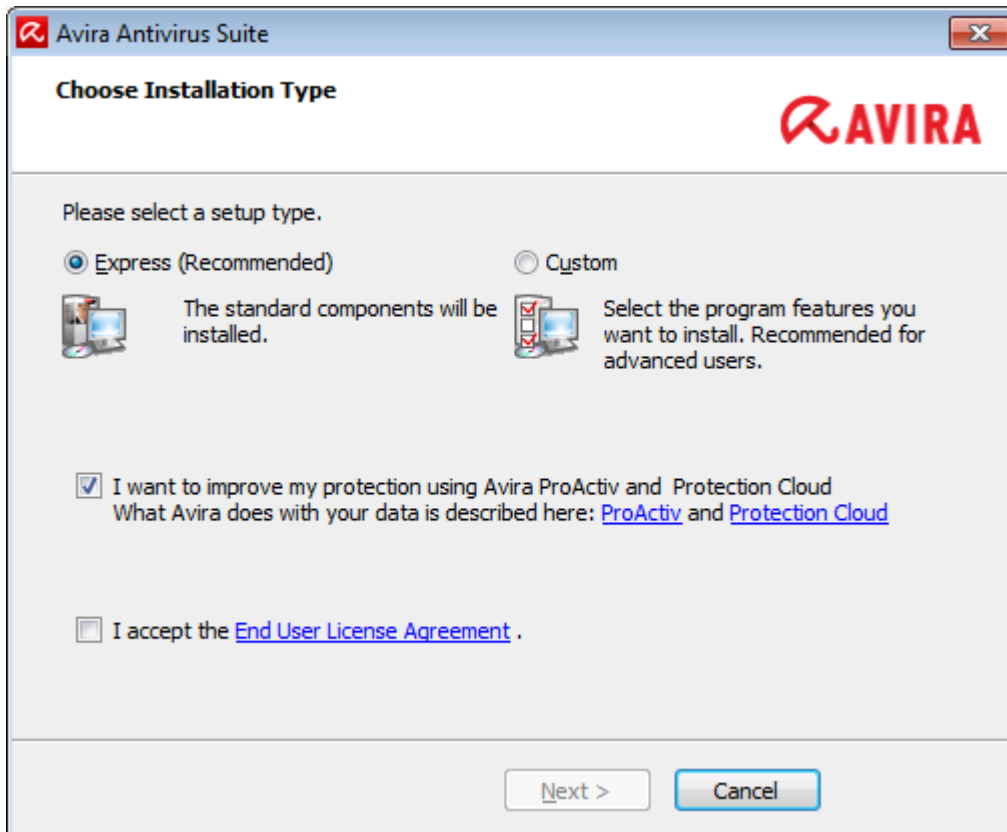
### 3.1 Installation and uninstallation

This chapter contains information relating to the installation of Avira Antivirus Suite.

- Preparing for installation
- Installing from CD when online
- Installing from CD when offline
- Installing downloaded software
- Removing incompatible software
- [Choosing an installation type](#)
- Installing Avira Antivirus Suite
- Changing the installation
- Uninstalling Avira Antivirus Suite

### 3.2 Choosing an installation type

During installation you can select a setup type in the installation wizard. The installation wizard is designed to smoothly guide you through the installation.



Related Topics:

- see [Performing an Express Installation](#)
- see [Performing a Custom Installation](#)

### 3.3 Pre-Setup

#### Note

Before installation, check whether your computer fulfills all the [minimum system requirements](#). If your computer satisfies all requirements, you can install the Avira product.

#### Pre-Setup

- ✓ Close your email program. It is also recommended to end all running applications.
- ✓ Make sure that no other virus protection solutions are installed. The automatic protection functions of various security solutions may interfere with each other.
  - The Avira product will search for any possible incompatible software on your computer.
  - If potentially incompatible software is detected Avira generates a list of these programs.



- It is recommended to remove these software programs in order not to endanger the stability of your computer.
- ▶ Select from the list the check boxes of all those programs that should be removed automatically from your computer and click **Next**.
- ▶ You have to confirm manually the uninstallation of some programs. Select the programs and click **Next**.
  - The uninstallation of one or more of the selected programs requires a restart of your computer. After rebooting the installation will continue.

**Warning**

Your computer will not be protected until the installation of the Avira product is finished.

**Installation**

The installation program runs in self-explanatory dialog mode. Every window contains a certain selection of buttons to control the installation process.

The most important buttons are assigned the following functions:

- **OK:** Confirm action.
- **Abort:** Abort action.
- **Next:** Go to next step.
- **Back:** Go to previous step.
- ▶ Establish an Internet connection: The Internet connection is necessary for performing the following installation steps:
  - Downloading the current program file and scan engine as well as the latest virus definition files via the installation program (for Internet-based installation)
  - Activating the program
  - Where appropriate, carrying out an update after completed installation
- ▶ Keep the activation code or license file for your Avira product handy when you want to activate the program.

**Note****Internet-based installation:**

For the Internet-based installation of the program, an installation program is provided that loads the current program file prior to installation by the Avira web servers. This process ensures that your Avira product is installed with the latest virus definition file.

**Installation with an installation package:**

The installation package contains both the installation program and all necessary

program files. No language selection for your Avira product is available for installation with an installation package. We recommend that you carry out an update of the virus definition file after installation.

#### Note

For product activation, your Avira product uses the HTTP protocol and Port 80 (web communication), as well as encryption protocol SSL and port 443, to communicate with the Avira servers. If you are using a firewall, please ensure that the required connections and/or incoming or outgoing data are not blocked by the firewall.

## 3.4 Performing an Express Installation

The *Express installation* is the recommended setup routine.

- It installs all the standard components of Avira Antivirus Suite. The Avira recommended security level settings are used.
- As default one of the following installation paths is chosen:
  - C:\Program Files\Avira (for Windows 32bit versions) or
  - C:\Program Files (x86)\Avira (for Windows 64bit versions)
- Here you can find all files related to Avira Antivirus Suite.
- If you choose this installation type, you can perform an installation by simply clicking **Next** until completion.
- This installation type is designed especially for those users who do not feel comfortable with configuring software tools.

## 3.5 Performing a Custom Installation

The *Custom installation* enables you to configure your installation. This is only recommended for advanced users who are well acquainted with matters of hard- and software as well as security issues.

- You can choose to install individual program components.
- A target folder can be selected for the program files to be installed.
- You can disable **Create a desktop icon and program group in the Start menu.**
- Using the configuration wizard, you can define custom settings for your Avira Antivirus Suite. Also you can choose the security level that you feel comfortable with.
- After installation you can initiate a short system scan that is performed automatically after installation.

## 3.6 Test product installation

Installing your Avira product:

Start the installation program by double-clicking the installation file you have downloaded from the Internet or insert the program CD.

### Internet-based installation

- The **Welcome** screen appears.
- ▶ Click **Next** to continue with the installation.
  - The dialog **Language selection** appears.
- ▶ Select the language you want to use to install your Avira product and confirm your language selection by clicking **Next**.
  - The dialog box **Download** appears. All files necessary for installation are downloaded from the Avira web servers. The **Download** window closes after conclusion of the download.

### Installation with an installation package

- The window **Preparing installation** appears.
- The installation file is extracted. The installation routine is started.
- The dialog box **Choose installation type** appears.

#### Note

By default **Express installation** is preset. All standard components will be installed which you may not configure. If you would like to execute an Custom installation, please refer to the chapter: [Installation and uninstallation > Custom installation](#).

- ▶ The **I want to improve my protection by using Avira Proactiv and Protection Cloud** check box ([Configuration > General > Advanced Protection](#)) is preset by default. If you do not want to participate in the Avira Community, please unmark this checkbox.
  - If you confirm your participation in the Avira Community, Avira sends data on detected suspicious programs to the Avira Malware Research Center. The data is used only for an advanced online scan and to expand and refine detection technology. You can click the links **ProActiv** and **Protection Cloud** to obtain more details on the expanded online and cloud scan.
- ▶ Confirm that you accept the **End User License Agreement**. For reading the detailed text of the **End User License Agreement**, click the corresponding link.
- ▶ Click **Next**.
  - The **License Wizard** opens and helps you to activate your product.

- You have the opportunity to configure a **Proxy server** right here.
- ▶ Click **Proxy settings** for configuration and confirm your settings with **OK**.
- ▶ Select the option **Test product** in the License Wizard and click **Next**.
- ▶ Insert your data into the required fields of **Registration**. Please decide whether to subscribe to the **Avira Newsletter** and click **Next**.
  - The installation progress is displayed by a green bar.
  - The dialog box **Join the millions of Avira users who already use Avira SearchFree Toolbar** appears.
- ▶ If you do not want to install the Avira SearchFree Toolbar, please unmark the checkbox with the Avira SearchFree Toolbar and the Avira SearchFree Updater **End User License Agreement**, and the one that defines **Avira SearchFree (search.avira.com)** as your browser homepage.

**Note**

If necessary, please uninstall any previously installed search toolbars before you install the Avira SearchFree Toolbar. Otherwise you will not be able to install the Avira SearchFree Toolbar.

- ▶ Click **Next**.
  - The installation progress of the Avira SearchFree Toolbar is displayed by a green bar.
- ▶ You will be asked to restart your system in order to activate your Avira product. Click **Yes** to reboot your computer immediately.
  - The Avira Tray Icon is placed in the taskbar.
  - Your evaluation license is valid for 31 days.

## 3.7 Configuration Wizard

At the end of a user-defined installation, the configuration wizard is opened. The configuration wizard enables you to define custom settings for your Avira product.

- ▶ Click **Next** in the welcome window of the configuration wizard to begin configuration of the program.
  - The **Configure AHeAD** dialog box enables you to select a detection level for the AHeAD technology. The detection level selected is used for the System Scanner (On-demand scan) and Real-Time Protection (On-access scan) AHeAD technology settings.
- ▶ Select a detection level and continue the installation by clicking **Next**.
  - In the following dialog box **Select extended threat categories**, you can adapt the protective functions of your Avira product to the threat categories specified.

- ▶ Where appropriate, activate further threat categories and continue the installation by clicking **Next**.
  - ➔ If you have selected the Avira Real-Time Protection installation module, the **Real-Time Protection start mode** dialog box appears. You can stipulate the Real-Time Protection start time. At each computer reboot, the Real-Time Protection will be started in the start mode specified.

**Note**

The specified Real-Time Protection start mode is saved in the registry and cannot be changed via Configuration.

**Note**

If the default start mode for Real-Time Protection (Normal start) has been chosen and the logon process upon startup is carried out fast, programs configured to start automatically upon startup might not be scanned, because they might be up and running before the Real-Time Protection has been started completely.

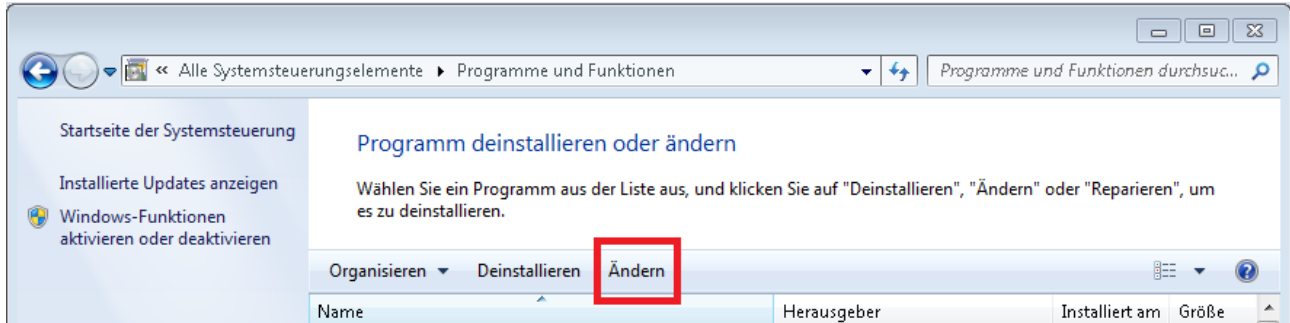
- ▶ Enable the required option and continue the configuration by clicking **Next**.
  - ➔ In the following **System scan** dialog box, a quick system scan can be enabled or disabled. The quick system scan is performed after the configuration has been completed and before the computer is rebooted, and scans running programs and the most important system files for viruses and malware.
- ▶ Enable or disable the **Quick system scan** option and continue the configuration by clicking **Next**.
  - ➔ In the following dialog box, you can complete the configuration by clicking **Finish**
  - ➔ The specified and selected settings are accepted.
  - ➔ If you have enabled the **Quick system scan** option, the **Luke Filewalker** window opens. The Scanner performs a quick system scan.
- ▶ If you are asked to restart your computer after the scan, click **Yes** to ensure that your system is fully protected.

After a successful installation, we recommend that you check whether the program is up-to-date in the **Status** field of the **Control Center**.

- ▶ If your Avira product shows that your computer is not secure, click **Fix problem**.
  - ➔ The dialog **Restore protection** opens.
- ▶ Activate the preset options in order to maximize the security of your system.
- ▶ If appropriate, perform a complete system scan afterwards.

## 3.8 Changing an installation under Windows 7

You have the option of adding or removing individual program components of the Avira Antivirus Suite installation (see [Choosing installation components](#)).



If you wish to add or remove modules of the current installation, you can use the option **Add or Remove Programs** in the **Windows control panel** to **Change/Remove** programs.

- Open the **Control Panel** via the Windows **Start** menu.

Double click on **Programs and Features**.

Select Avira Antivirus Suite and click **Change**.

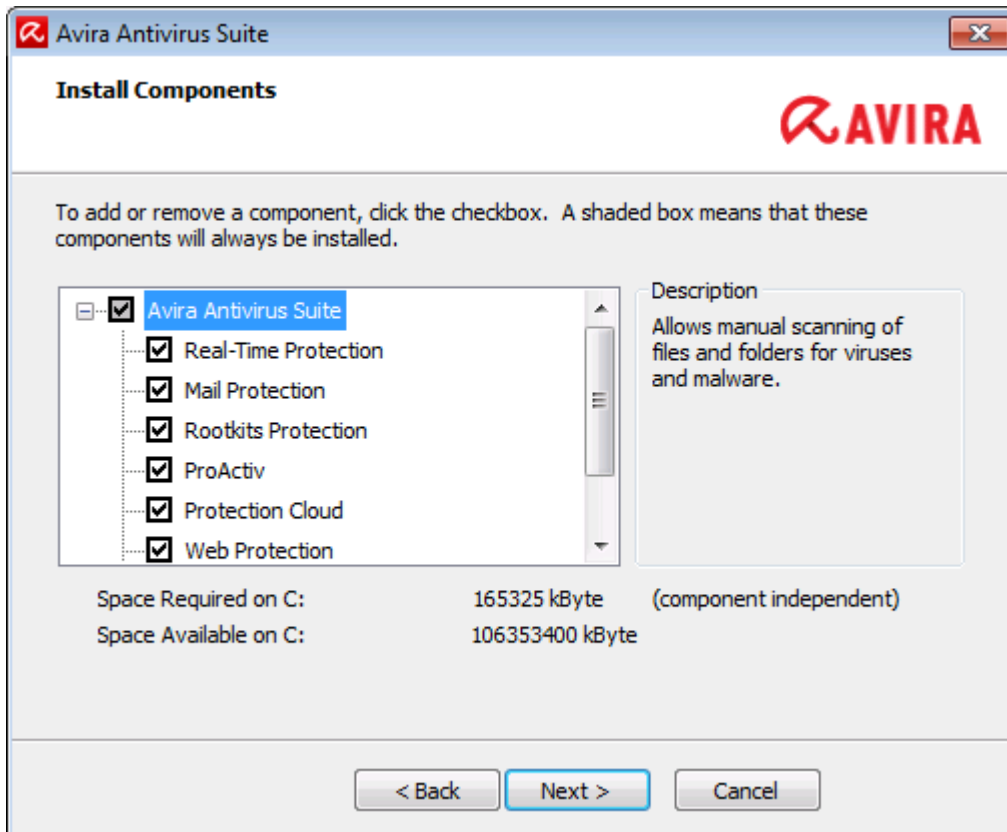
In the **Welcome** dialog of the program, select the option **Modify**. You will be guided through the installation changes.

Related Topics:

[Choosing installation components](#)

## 3.9 Choosing installation components

In a custom installation or a change installation, the following installation components can be selected, added or removed.



Select or deselect components from the list in the Install components dialog.

- **Avira Antivirus Suite**

This contains all components required for successful installation of Avira Antivirus Suite.

- **Real-Time Protection**

The Avira Real-Time Protection runs in the background. It monitors and repairs, if possible, files during operations such as open, write and copy in "on-access mode". On access mode means that, whenever a user carries out a file operation (e.g. load document, execute, copy), Avira Antivirus Suite automatically scans the file. Renaming a file, however, does not trigger a scan by Avira Real-Time Protection.

- **Mail Protection**

Mail Protection is the interface between your computer and the email server from which your email program (email client) downloads emails. Mail Protection is connected as a so-called proxy between the email program and the email server. All incoming emails are routed through this proxy, scanned for viruses and unwanted programs and forwarded to your email program. Depending on the configuration, the program processes the affected emails automatically or asks you for a certain action.

- **Windows Firewall** (starting from Windows Vista)

This component manages the Windows Firewall from Avira Antivirus Suite.

- **Rootkits Protection**

Avira Rootkits Protection checks whether software is already installed on your computer that can no longer be detected with conventional methods of malware protection after penetrating the computer system.

- **ProActiv**

The ProActiv component monitors application actions and alerts users to suspicious



application behavior. This behavior-based recognition enables you to protect yourself against unknown malware. The ProActiv component is integrated into Avira Real-Time Protection.

- **Protection Cloud**

The Protection Cloud component is a module for dynamic online detection of still unknown malware. This means that the files are uploaded to a remote location and compared to known files as well as other files that are being uploaded and analyzed in real-time (unscheduled and without delay). This way the database is constantly updated, therefore an even higher level of security can be provided.

If you have chosen to install the Protection Cloud component, but you want to confirm manually, which files should be sent to the Cloud for analysis, you can enable the option **Confirm manually when sending suspicious files to Avira**.

- **Web Protection**

When surfing the Internet, you are using your web browser to request data from a web server. The data transferred from the web server (HTML files, script and image files, Flash files, video and music streams, etc.) will normally be moved directly into the browser cache for display in the web browser, meaning that an on-access scan as performed by Avira Real-Time Protection is not possible. This could allow viruses and unwanted programs to access your computer system. Web Protection is what is known as an HTTP proxy which monitors the ports used for data transfer (80, 8080, 3128) and scans the transferred data for viruses and unwanted programs.

Depending on the configuration, the program may process the affected files automatically or prompt the user for a specific action.

- **Shell Extension**

The Shell Extension generates an entry **Scan selected files with Avira** in the context menu of the Windows Explorer (right-hand mouse button). With this entry you can directly scan files or directories.

### **Related Topics:**

Changing an installation

## **3.10 Uninstallation**

If you wish to remove the Avira product from your computer, you can use the option **Add or Remove Programs** to **Change/Remove** programs in the Windows Control Panel.

To uninstall your Avira product (e.g. in Windows 7):

- ▶ Open the **Control Panel** via the Windows **Start** menu.
- ▶ Double click on **Programs and Features**.
- ▶ Select your Avira product in the list and click **Uninstall**.
  - You will be asked if you really want to remove the program.
- ▶ Click **Yes** to confirm.
  - All components of the program will be removed.



- ▶ Click **Finish** to complete uninstallation.
  - Where appropriate, a dialog box appears recommending that your computer be restarted.
- ▶ Click **Yes** to confirm.
  - The Avira product is now uninstalled and all directories, files and registry entries for the program are deleted when your computer is restarted.

**Note**

The Avira SearchFree Toolbar is not included in the uninstallation program and must be uninstalled separately by following the steps detailed above. To do this in Firefox the Avira SearchFree Toolbar must be enabled via the Add-On Manager. After uninstallation the search toolbar is no longer integrated in your web browser.

## 4. Overview of Avira Antivirus Suite

This chapter contains an overview of the functionality and operation of your Avira product.

- see Chapter [User interface and operation](#)
- see Chapter [Avira SearchFree Toolbar](#)
- see Chapter [How to...?](#)

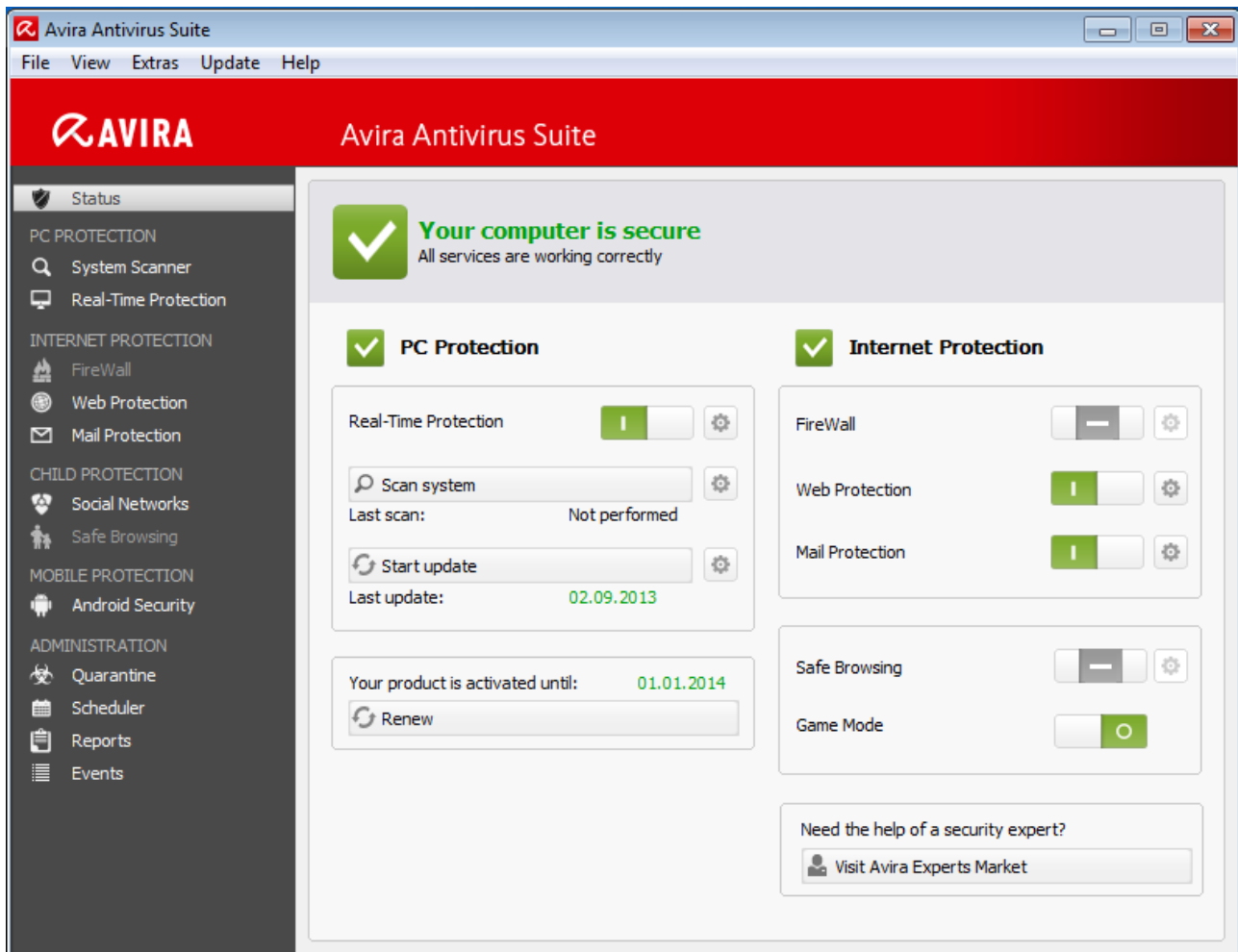
### 4.1 User interface and operation

You operate your Avira product via three program interface elements:

- [Control Center](#): monitoring and controlling the Avira product
- [Configuration](#): Configuring the Avira product
- [Tray Icon](#) in the system tray of the taskbar: Opening the Control Center and other functions

#### 4.1.1 Control Center

The Control Center is designed to monitor the protection status of your computer systems and control and operate the protection components and functions of your Avira product.



The Control Center window is divided into three areas: The **Menu bar**, the **Navigation area** and the detail window **Status**:

- **Menu bar:** In the Control Center menu bar, you can access general program functions and information on the program.
- **Navigation area:** In the navigation area, you can easily swap between the individual sections of the Control Center. The individual sections contain information and functions of the program components and are arranged in the navigation bar according to activity. Example: Activity *PC PROTECTION* - Section **Real-Time Protection**.
- **Status:** The Control Center opens with the **Status** view, where you can see at a glance, if your computer is safe, and you have an overview of the active modules and the date of the last system scan. The **Status** view also contains buttons for starting features or actions, such as starting or stopping the **Real-Time Protection**.

### Starting and closing of Control Center

To start the Control Center the following options are available:

- Double-click the program icon on your desktop
- Via the program entry in the **Start > Programs** menu.
- Via the Tray Icon of your Avira product.

Close the Control Center via the menu command **Close** in the menu **File** or by clicking on the close tab in the Control Center.

## Operate Control Center

To navigate in the Control Center

- ▶ Select an activity in the navigation bar.
  - ➔ The activity opens and other sections appear. The first section of the activity is selected and displayed in the view.
- ▶ If necessary, click another section to display this in the detail window.

### Note

You can activate the keyboard navigation in the menu bar with the help of the **[Alt]** key. If navigation is activated, you can move within the menu with the **arrow** keys. With the **Return** key you activate the active menu item. To open or close menus in the Control Center, or to navigate within the menus, you can also use the following key combinations: **[Alt]** + underlined letter in the menu or menu command. Hold down the **[Alt]** key if you want to access a menu, a menu command or a submenu.

To process data or objects displayed in the detail window:

- ▶ Highlight the data or object you wish to edit.
  - To highlight multiple elements (elements in columns), hold down the **control** key or the **shift** key while selecting the elements.
- ▶ Click the appropriate button in the upper bar of the detail window to edit the object.

## Control Center overview

- **Status:** Clicking on the **Status** bar gives you an overview of the product's functionality and performance (see Status).
  - The **Status** section lets you see at a glance which modules are active and provides information on the last update performed.
- **PC PROTECTION:** In this section you will find the components for checking the files on your computer system for viruses and malware.
  - The System Scanner section enables you to easily configure and start an on-demand scan. Predefined profiles enable a scan with already adapted default options. In the same way it is possible to adapt the scan for viruses and unwanted programs to your personal requirements with the help of manual selection (will be saved) or by creating user-defined profiles.
  - The Real-Time Protection section displays information on scanned files, as well as other statistical data, which can be reset at any time, and enables access to the report file. More detailed information on the last virus or unwanted program detected can be obtained practically "at the push of a button".

- The FireWall section enables you to configure the basic settings for the FireWall. In addition, the current data transfer rate and all active applications using a network connection are displayed.
- The Web Protection section displays information on scanned URLs and detected viruses, as well as other statistical data, which can be reset at any time and enables access to the report file. More detailed information on the last virus or unwanted program detected can be obtained practically "at the push of a button".
- The Mail Protection section shows you all the emails scanned by Mail Protection, their properties and other statistical data. You can also exclude email addresses from future scanning for malware or spam.
- *CHILD PROTECTION*: In this section you will find the components to ensure a safe Internet experience for your children.
  - Social Networks: This section redirects you to the Social Network Protection application. Social Network Protection informs parents of their children's activities online. It checks their social network accounts for comments, photos etc. that may influence the child's reputation in a negative way or may indicate that the child is in danger.
- *MOBILE PROTECTION*: From this section you will be redirected to the online access for Android devices.
  - Avira Android Security manages all your android-based devices.
- *ADMINISTRATION*: In this section you will find tools for isolating and managing suspicious or infected files, and for planning recurring tasks.
  - The Quarantine section contains the so-called quarantine manager. This is the central point for files already placed in quarantine or for suspect files that you would like to place in quarantine. It is also possible to send a selected file to the Avira Malware Research Center by email.
  - The Scheduler section enables you to configure scheduled scanning and update jobs as well as backup jobs and to adapt or delete existing jobs.
  - The Reports section enables you to view the results of actions performed.
  - The Events section enables you to view events generated by certain program modules.

#### 4.1.2 Game Mode

If an application is executed in full-screen mode on your computer system, you may intentionally suspend desktop notifications as pop-up windows and in-product messages by activating the Game Mode.

You may enable the Game Mode or keep it in automatic mode by clicking the **ON/OFF** button. By default the Game Mode is set to **automatic** and displayed in green color. The default setting sets the feature to automatic, so that whenever you run an application that needs the full-screen mode, your Avira product switches automatically to Game Mode.

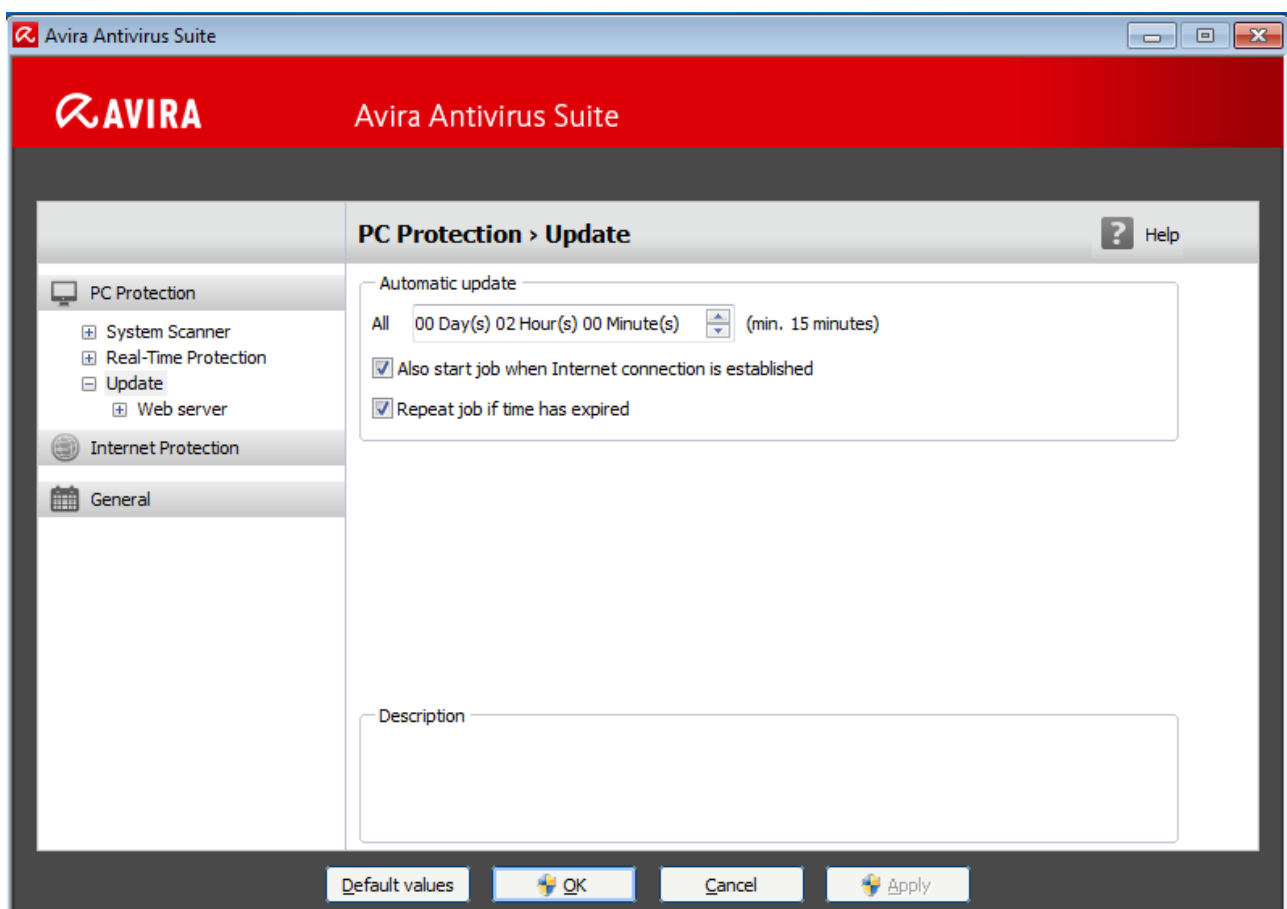
- ▶ Click the button on the left next to the **OFF** button to activate the Game Mode.
  - ➔ The Game Mode is enabled and displayed in yellow color.

### Note

We recommend to change the default setting **OFF** with its automatic full-screen recognition mode only temporarily, because you won't receive visible desktop notifications and warnings concerning network events and possible threats.

## 4.1.3 Configuration

You can define settings for your Avira product in the Configuration. After installation, your Avira product is configured with standard settings, ensuring optimal protection for your computer system. However, your computer system or your specific requirements for your Avira product may mean you need to adapt the protective components of the program.



The Configuration opens a dialog box: You can save your configuration settings via the **OK** or **Apply** buttons, delete your settings by clicking the **Cancel** button or restore your default configuration settings using the **Default values** button. You can select individual configuration sections in the left-hand navigation bar.

### Accessing the Configuration

You have several options for accessing the configuration:

- via the Windows control panel.

- via the Windows Security Center - from Windows XP Service Pack 2.
- via the Tray Icon of your Avira product.
- in the Control Center via the menu item Extras > Configuration.
- in the Control Center via the Configuration button.

**Note**

If you are accessing configuration via the **Configuration** button in the Control Center, go to the Configuration register of the section which is active in the Control Center.

**Configuration operation**

Navigate in the configuration window as you would in Windows Explorer:

- ▶ Click an entry in the tree structure to display this configuration section in the detail window.
- ▶ Click the plus symbol in front of an entry to expand the configuration section and display configuration subsections in the tree structure.
- ▶ To hide configuration subsections, click on the minus symbol in front of the expanded configuration section.

**Note**

To enable or disable Configuration options and use the buttons, you can also use the following key combinations: **[Alt]** + underlined letter in the option name or button description.

If you want to confirm your Configuration settings:

- ▶ Click **OK**.
  - The configuration window is closed and the settings are accepted.
- OR -
- ▶ Click **Apply**.
  - The settings are applied. The configuration window remains open.

If you want to finish configuration without confirming your settings:

- ▶ Click **Cancel**.
  - The configuration window is closed and the settings are discarded.

If you want to restore all configuration settings to default values:

- ▶ Click **Default values**.

- All settings of the configuration are restored to default values. All amendments and custom entries are lost when default settings are restored.

## Overview of configuration options

The following configuration options are available:



- **System Scanner:** Configuration of on-demand scan
  - Scan options
  - Action on detection
  - Archive scan options
  - System scan exceptions
  - System scan heuristics
  - Report function setting
- **Real-Time Protection:** Configuration of on-access scan
  - Scan options
  - Action on detection
  - Further actions
  - On-access scan exceptions
  - On-access scan heuristics
  - Report function setting
- **Update:** Configuration of the update settings
  - Proxy settings
- **Web Protection:** Configuration of Web Protection
  - Scan options, enabling and disabling the Web Protection
  - Action on detection
  - Blocked access: Unwanted file types and MIME types, Web filter for known unwanted URLs (malware, phishing, etc.)
  - Web Protection scan exceptions: URLs, file types, MIME types
  - Web Protection heuristics
  - Report function setting
- **Mail Protection:** Configuration of Mail Protection
  - Scan options: Enable the monitoring of POP3 accounts, IMAP accounts, outgoing emails (SMTP)
  - Actions on detection
  - Further actions
  - Mail Protection scan heuristics
  - AntiBot function: Permitted SMTP servers, permitted email senders
  - Mail Protection scan exceptions
  - Configuration of cache, empty cache



- Report function setting
- **General:**
  - Threat categories for System Scanner and Real-Time Protection
  - Advanced protection: Options to enable the ProActiv and Protection Cloud features.
  - Application filter: Block or allow applications
  - Password protection for access to the Control Center and the Configuration
  - Security: block autostart function, product protection, protect Windows hosts file
  - WMI: Enable WMI support
  - Event log configuration
  - Configuration of report functions
  - Setting of directories used
  - Configuration of acoustic alerts when malware is detected

#### 4.1.4 Tray icon

After installation, you will see the tray icon of your Avira product in the system tray of the taskbar:

Icon	Description
	Avira Real-Time Protection is enabled
	Avira Real-Time Protection is disabled

The tray icon displays the status of the Real-Time Protection service.

Central functions of your Avira product can be quickly accessed via the context menu of the **tray icon**. To open the context menu, click the **tray icon** with the right-hand mouse button.

##### Entries in the context menu

- **Enable Real-Time Protection:** Enables or disables the Avira Real-Time Protection.
- **Enable Mail Protection:** Enables or disables the Avira Mail Protection.
- **Enable Web Protection:** Enables or disables the Avira Web Protection.
  - **Enable Windows Firewall:** Enables or disables the Windows Firewall (this feature is available starting from Windows 8).
- **Start Avira Antivirus Suite:** Opens the Control Center.
- **Configure Avira Antivirus Suite:** Opens the Configuration.

- **My messages:** Opens a slide-up with the current information about your Avira product.
- **My communication settings:** Opens the Product Message Subscription Center
- **Start update:** Starts an update.
- **Help:** opens the Online Help.
- **Experts Market - Ask for help:** opens the Experts Market - Ask for help website where you can ask for help or offer your help to other users.
- **About Avira Antivirus Suite:** Opens a dialog box with information on your Avira product: Product information, Version information, License information.
- **Avira on the Internet:** Opens the Avira web portal on the Internet. The condition for this is that you have an active connection to the Internet.

**Note**

The User Account Control (UAC) will ask for your permission to enable or disable the Real-Time Protection, Web Protection and Mail Protection services in operating systems as of Windows Vista.

## 4.2 Avira SearchFree Toolbar

Avira SearchFree Toolbar includes two main components: Avira SearchFree and the Toolbar.

The Avira SearchFree Toolbar is installed as an add-on. When the browser is first accessed (in Firefox and Internet Explorer) a message will pop-up, asking you for permission to install the toolbar. You will have to accept in order to complete a successful installation of Avira SearchFree Toolbar.

Avira SearchFree is a search engine and contains a clickable Avira logo linked to the Avira website and web, image and video channels. This allows Avira users a safer Internet navigation.

The toolbar, integrated in your web browser, consists of a search box, an Avira logo linked to the Avira website, two status displays, three widgets and the **Options** menu.

- **Search toolbar**  
Use the search toolbar for free to quickly search the Internet using the Avira search engine.
- **Status display**  
The status displays provide information on the status of the Web Protection and the current update status of your Avira product and helps you identify which actions you need to take to protect your PC.
- **Widgets**  
Avira offers you three widgets to the most important Internet-related functions. With one click you have direct access to Facebook and your email, or you can ensure safe web browsing (Firefox and Internet Explorer only).

- [Options](#)

You can use the **Options** menu to access the toolbar options, clear the history, find toolbar help and information and also uninstall the Avira SearchFree Toolbar directly via the web browser (Firefox and Internet Explorer only).

#### 4.2.1 Use

##### Avira SearchFree

You can use Avira SearchFree to define any number of terms to browse the Internet.



Enter the term in the search box and press the **Enter** key or click on **Search**. The Avira SearchFree engine then searches the Internet for you and displays all hits in the browser window.



To find out how to custom configure Avira SearchFree in Internet Explorer, Firefox and Chrome, go to [Options](#).

##### Status display

##### Web Protection

You can use the following icons and messages to identify which actions you need to take to protect your PC:

Icon	Status display	Description
	<i>Web Protection</i>	If you move the cursor over the icon, the following message appears: <i>Avira Web Protection is active. Your browsing is protected.</i>  No further action is necessary.
	<i>Web Protection is inactive</i>	If you move the cursor over the icon, the following message appears: <i>Avira Web Protection is off. Click to find out how to turn it on.</i>  → You will be redirected to one of our Knowledge Base articles.

	<i>No Web Protection</i>	<p>If you move the cursor over the icon, one of the following messages appears:</p> <ul style="list-style-type: none"> <li><i>You do not have Avira Web Protection installed. Click to find out how to protect your browsing.</i></li> </ul> <p>This message will appear if you install incorrectly or uninstall the Avira Antivirus.</p> <ul style="list-style-type: none"> <li><i>Web Protection is included for free with Avira Antivirus. Click to find out how to install it.</i></li> </ul> <p>This message will appear if you do not install Web Protection or if you uninstall it.</p> <ul style="list-style-type: none"> <li>→ In both cases, you will be redirected to the Avira homepage, where you can download the Avira product .</li> </ul>
	<i>Error</i>	<p>If you move the cursor over the icon, the following message appears: <i>Avira reported an error. Click to contact Support for help.</i></p> <ul style="list-style-type: none"> <li>► Click the gray icon or text to go to the Avira Support page.</li> </ul>

## Widgets

Avira SearchFree contains three widgets with the most important functions for the nowadays Internet web browsing: Facebook, E-mail and Browser Security.

### Facebook

This function allows you to receive all the messages from Facebook and to be always updated.

### Email

If you click the email symbol in the toolbar, a dropdown list will be shown. You can choose between the most commonly used email providers.

### Browser Security

This widget has been conceived to offer you in one click all the Internet security options

you may need on daily basis. This option is only available for Firefox and Internet Explorer. Also the names of the functions sometimes change from one browser to another:

- *Pop-up Blocker*

If this option is activated, all pop-up windows will be blocked.

- *Block Cookies*

If you activate this option, no cookies will be saved on your computer.

- *Private Browsing (Firefox) / InPrivate Browsing (Internet Explorer)*

Enable this option if you do not want to leave any personal information on the Internet while you surf. This option is not available for Internet Explorer 7 and 8.

- *Clear Recent History (Firefox) / Delete Browsing History (Internet Explorer)*

With this option you will erase all traces of your Internet activities.






## Website Safety Advisor

The Website Safety Advisor offers you a safety ranking while navigating.

You can assess the reputation of the website you are visiting, and check if it poses a low or a high risk to your security.

This widget also provides further information on the website, like who is the domain owner, or why the website has been categorized as safe or risky.

The status of the Website Safety Advisor is displayed in the Toolbar and in your search results, as an Avira tray icon in combination with other icons:

Icon	Status display	Description
	<i>Safe</i>	A green check mark for safe websites.
	<i>Low risk</i>	A yellow exclamation mark for websites representing a low risk.
	<i>High risk</i>	A red stop sign for websites representing a high risk to your security.
	<i>Unknown</i>	A grey question mark will appear when the status is unknown.
	<i>Verifying</i>	This sign will appear while verifying the status of a website.

## Browser Tracking Blocker

With the Browser Tracking Blocker you can stop trackers from collecting information about

you while you are surfing.

The widget allows you to choose which trackers to block and which ones to allow.

The tracking companies are classified in three categories:

- Social Networks
- Ad Networks
- Other companies

## 4.2.2 Options

Avira SearchFree Toolbar is compatible with Internet Explorer, Firefox and Google Chrome and can be configured in the three web browsers:

- [Internet Explorer configuration options](#)
- [Firefox configuration options](#)
- [Google Chrome configuration options](#)

### Internet Explorer

In Internet Explorer, the following configuration options for the Avira SearchFree Toolbar are available in the **Options** menu:

### Toolbar options

#### Search

##### Avira search engine

In the **Avira search engine** menu, you can select which search engine to use for the search. Search engines are available for the USA, Brazil, Germany, Spain, Europe, France, Italy, the Netherlands, Russia and the United Kingdom.

##### Open searches in

In the **Open searches in** option menu, you can select where the search result should be displayed; in the Current window, in a New window or on a New tab.

##### Display recent searches

If the **Display recent searches** option is enabled, you can display previous search terms under the text entry box of the search toolbar.

##### Auto clear recent search history when I close the browser

Enable the option **Auto clear recent search history when I close the browser** if you do not want to save previous searches and want to clear the history when you close the web browser.

## More options

### Select toolbar language

Under **Select toolbar language** you can select the language in which Avira SearchFree Toolbar is displayed. The toolbar is available in English, German, Spanish, French, Italian, Portuguese and Dutch.

#### Note

Where possible, the default Avira SearchFree Toolbar language corresponds to that of your program. If the toolbar is not available in your language, the default language is English.

### Show button text labels

Disable the **Show button text labels** option if you want to hide the text next to the Avira SearchFree Toolbar icons.

## Clear history

Enable the **Clear history** option if you do not want to save previous searches and want to clear the history immediately.

## Help

Click on **Help** to access the website containing frequently asked questions (FAQs) relating to the toolbar.

## Uninstall

You can also uninstall Avira SearchFree Toolbar directly in Internet Explorer:  
Uninstallation via the web browser

## About

Click on **About** to display which version of Avira SearchFree Toolbar is installed.

## Firefox

In the Firefox web browser, the following configuration options for the Avira SearchFree Toolbar are available in the **Options** menu:

## Toolbar options

### Search

#### Select Avira search engine

In the **Avira search engine** menu, you can select which search engine to use for the search. Search engines are available for the USA, Brazil, Germany, Spain, Europe, France, Italy, the Netherlands, Russia and the United Kingdom.

#### Display recent searches

If the **Display recent searches** option enabled, you can display previous search terms by clicking on the arrow in the search toolbar. Select a term if you want to display the search result again.

#### Auto clear recent search history when I close the browser

Enable the option **Auto clear recent search history when I close the browser** if you do not want to save previous searches and want to clear the history when you close the web browser.

#### Display Avira search results when I type keywords or invalid URLs into the browser address bar

If this option is enabled, a search is initiated and the search result displayed every time you enter keywords or an invalid URL into the web browser's address bar.

### More options

#### Select toolbar language

Under **Select toolbar language** you can select the language in which Avira SearchFree Toolbar is displayed. The toolbar is available in English, German, Spanish, French, Italian, Portuguese and Dutch.

#### Note

Where possible, the default Avira SearchFree Toolbar language corresponds to that of your program. If the toolbar is not available in your language, the default language is English.

#### Show button text labels

Disable the **Show button text labels** option if you want to hide the text next to the Avira SearchFree Toolbar icons.

### Clear history

Enable the **Clear history** option if you do not want to save previous searches and want to clear the history immediately.



## Help

Click on **Help** to access the website containing frequently asked questions (FAQs) relating to the toolbar.

## Uninstall

You can also uninstall Avira SearchFree Toolbar directly in Firefox: Uninstallation via the web browser.

## About

Click on **About** to display which version of Avira SearchFree Toolbar is installed.

## Google Chrome

In the Chrome web browser, the following configuration options for Avira SearchFree Toolbar are available under the menu of the red Avira umbrella:

## Help

Click on **Help** to access the website containing frequently asked questions (FAQs) relating to the toolbar.

## Uninstall instructions

Here you will be linked to the articles that contain all the information you need to uninstall the toolbar.

## About

Click on **About** to display which version of the Avira SearchFree Toolbar is installed.

## Show/ Hide the Avira SearchFree Toolbar

Click here to hide or show Avira SearchFree Toolbar on your web browser.

### 4.2.3 Uninstalling Avira SearchFree Toolbar under Windows 7

To uninstall your Avira SearchFree Toolbar:

- Close your web browser.

Open the **Control Panel** via the Windows **Start** menu.

Double click on **Programs and Features**.

Select Avira SearchFree Toolbar plus Web Protection in the list and click **Uninstall**.

You will be asked if you really want to uninstall this product.

Click **Yes** to confirm.

Avira SearchFree Toolbar plus Web Protection is uninstalled and all directories, files and registry entries for the Avira SearchFree Toolbar plus Web Protection are deleted when your computer is restarted.

## 4.3 How to...?

The chapters "How to...?" offer short instructions about license and product activation as well as information on the most important functions of your Avira product. The selected short articles serve as an overview about the functionality of your Avira product. They do not substitute the detailed information of each section of this help center.

### 4.3.1 Activate license

#### **To activate your Avira product's license:**

Activate your license for your Avira product with the **.KEY** license file. You can obtain the license file by email from Avira. The license file contains the license for all products that you have ordered in one order process.

If you have not yet installed your Avira product:

- ▶ Save the license file to a local directory on your computer.
- ▶ Install your Avira product.
- ▶ During installation, enter the save location of the license file.

If you have already installed your Avira product:

- ▶ Double-click the license file in File Manager or in the activation email and follow the on-screen instructions when License Manager opens.

- OR -

In your Avira product's Control Center, select the menu item **Help > License management**

#### **Note**

As of Windows Vista the User Account Control dialog box appears. Log in as administrator if appropriate. Click **Continue**.

- ▶ Highlight the license file and click **Open**.
  - ↪ A message appears.
- ▶ Click **OK** to confirm.
  - ↪ The license is activated.
- ▶ If necessary, restart your system.

### 4.3.2 Activate product

To activate your Avira product, you have the following options:

#### Activation with a valid full license

To activate the program with a full license, you need a valid activation code, which holds data of the license you have purchased. You have received the activation code from us either by email or it has been printed on the product packaging.

#### Activation with an evaluation license

Your Avira product is activated with an automatically generated evaluation license, with which you can test the Avira product with its complete range of function for a limited period of time.

##### Note

For product activation or for a test license you need an active Internet link. If no connection can be established to the servers of Avira, please check the settings of the firewall used: Connections via the HTTP protocol and port 80 (web communication) and via the encryption protocol SSL and port 443 are used for product activation. Make sure that your firewall does not block incoming and outgoing data. First of all check whether you can access web pages with your web browser.

The following describes how to activate your Avira product:

If you have not yet installed your Avira product:

- ▶ Install your Avira product.
  - During the installation process you will be asked to select an activation option
- **Activate product:** Activation with a valid full license
- **Test product:** Activation with an evaluation license
- ▶ Enter the activation code for an activation with a full license.
- ▶ Acknowledge the selection of the activation procedure by clicking **Next**.
- ▶ If and when necessary, enter your personal data for registration and acknowledge by clicking **Next**.
  - Your license data will be displayed in the next window. Your Avira product has been enabled.
- ▶ Continue to install.


If you have already installed your Avira product:

- ▶ In the Control Center, select the menu item **Help > License management**.

- The *license wizard* opens, in which you can select an activation option. The next steps of product activation are identical with the procedure described above.

### 4.3.3 Perform automatic updates

To create a job with the Avira Scheduler to update your Avira product automatically:

- ▶ In the Control Center, select the section *ADMINISTRATION* > **Scheduler**.
- ▶ Click the  **Insert new job** icon.
  - The dialog box **Name and description of the job** appears.
- ▶ Give the job a name and, where appropriate, a description.
- ▶ Click **Next**.
  - The dialog box **Type of job** is displayed.
- ▶ Select **Update job** from the list.
- ▶ Click **Next**.
  - The dialog box **Time of job** appears.
- ▶ Select a time for the update:
  - **Immediately**
  - **Daily**
  - **Weekly**
  - **Interval**
  - **Single**
  - **Login**

#### Note

We recommend regular automatic updates. The recommended update interval is: 2 hours.

- ▶ Where appropriate, specify a date according to the selection.
- ▶ Where appropriate, select additional options (availability depends on type of job):
  - **Repeat job if time has expired**  
Past jobs are performed that could not be performed at the required time, for example because the computer was switched off.
  - **Start job while connecting to the Internet (dial-up)**  
In addition to the defined frequency, the job is performed when an Internet connection is set up.
- ▶ Click **Next**.
  - The dialog box **Select display mode** appears.
- ▶ Select the display mode of the job window:

- **Invisible:** No job window
- **Minimize:** progress bar only
- **Maximize:** Entire job window
- ▶ Click **Finish**.
  - Your newly created job appears on the start page of the *ADMINISTRATION > Scheduler* section with the status enabled (check mark).
- ▶ Where appropriate, deactivate jobs that are not to be performed.
- Use the following icons to further define your jobs:



View properties of a job



Edit job



Delete job



Start job



Stop job

#### 4.3.4 Start a manual update

You have various options for starting an update manually: When an update is started manually, the virus definition file and scan engine are always updated.

To start an update of your Avira product manually:

- ▶ With the right-hand mouse button, click the Avira tray icon in the taskbar.
  - A context menu appears.
- ▶ Select **Start update**.
  - The **Updater** dialog box appears.
- OR -
- ▶ In the Control Center, select **Status**.
- ▶ In the **Last update** field, click on the **Start update** link.
  - The Updater dialog box appears.
- OR -
- ▶ In the Control Center, in the **Update** menu, select the menu command **Start update**.
  - The Updater dialog box appears.

**Note**

We recommend regular automatic updates. The recommended update interval is: 2 hours.

**Note**

You can also carry out a manual update directly via the Windows security center.

### 4.3.5 Using a scan profile to scan for viruses and malware

A scan profile is a set of drives and directories to be scanned.

The following options are available for scanning via a scan profile:

**Use predefined scan profile**

If the predefined scan profile corresponds to your requirements.

**Customize and apply scan profile (manual selection)**

If you want to scan with a customized scan profile.

**Create and apply new scan profile**

If you want to create your own scan profile.

Depending on the operating system, various icons are available for starting a scan profile:

- In Windows XP:



This icon starts the scan via a scan profile.

- As of Windows Vista:

As of Microsoft Windows Vista, the Control Center only has limited rights at the moment, e.g. for access to directories and files. Certain actions and file accesses can only be performed in the Control Center with extended administrator rights. These extended administrator rights must be granted at the start of each scan via a scan profile.



- This icon starts a limited scan via a scan profile. Only directories and files that the operating system has granted access rights to are scanned.



- This icon starts the scan with extended administrator rights. After confirmation, all directories and files in the selected scan profile are scanned.

To scan for viruses and malware with a scan profile:

- ▶ Go to Control Center and select the section *PC PROTECTION* > **System Scanner**.

→ Predefined scan profiles appear.



- ▶ Select one of the predefined scan profiles.

-OR-

Adapt the scan profile **Manual selection**.

-OR-

Create a new scan profile

- ▶ Click the icon (Windows XP:  or as of Windows Vista:  ).
- ▶ The **Luke Filewalker** window appears and a system scan is started.
  - When the scan is completed, the results are displayed.


If you want to adapt a scan profile:


- ▶ In the scan profile **Manual Selection**, expand the file tree so that all the drives and directories you want to scan are open.
  - Click the + icon: The next directory level is displayed.
  - Click the - icon: The next directory level is hidden.
- ▶ Highlight the nodes and directories you want to scan by clicking on the relevant box of the appropriate directory level:

The following options are available for selecting directories:

- Directory, including sub-directories (black check mark)
- Sub-directories of one directory only (grey check mark, sub-directories have black check marks)
- No directory (no check mark)

If you want to create a new scan profile:

- ▶ Click the icon  **Create new profile**.
  - The profile **New profile** appears below the profiles previously created.

- ▶ Where appropriate, rename the scan profile by clicking on the icon .
- ▶ Highlight the nodes and directories to be saved by clicking the check box of the respective directory level.

The following options are available for selecting directories:

- Directory, including sub-directories (black check mark)
- Sub-directories of one directory only (grey check mark, sub-directories have black check marks)
- No directory (no check mark)

#### 4.3.6 Scan for viruses and malware using drag & drop

To scan for viruses and malware systematically using drag & drop:

- ✓ The Control Center of your Avira product has been opened.
- ▶ Highlight the file or directory you want to scan.
- ▶ Use the left-hand mouse button to drag the highlighted file or directory into the **Control Center**.
  - The **Luke Filewalker** window appears and a system scan is started.
  - When the scan is completed, the results are displayed.

#### 4.3.7 Scan for viruses and malware via the context menu

To scan for viruses and malware systematically via the context menu:


- ▶ Click with the right-hand mouse button (e.g. in Windows Explorer, on the desktop or in an open Windows directory) on the file or directory you want to scan.
  - The Windows Explorer context menu appears.
- ▶ Select **Scan selected files with Avira** in the context menu.
  - The **Luke Filewalker** window appears and a system scan is started.
  - When the scan is completed, the results are displayed.

#### 4.3.8 Automatically scan for viruses and malware

##### Note

After installation, the scan job **Full system scan** is created in the Scheduler: A complete system scan is automatically performed at a recommended interval.

To create a job to automatically scan for viruses and malware:

- ▶ In the Control Center, select the section *ADMINISTRATION* > **Scheduler**.
- ▶ Click the icon .
- The dialog box **Name and description of job** appears.
- ▶ Give the job a name and, where appropriate, a description.
- ▶ Click **Next**.
  - The dialog box **Type of job** appears.
- ▶ Select **Scan job**.
- ▶ Click **Next**.
  - The dialog box **Selection of the profile** appears.



- ▶ Select the profile to be scanned.
- ▶ Click **Next**.
  - The dialog box **Time of the job** appears.
- ▶ Select a time for the scan:
  - **Immediately**
  - **Daily**
  - **Weekly**
  - **Interval**
  - **Single**
  - **Login**
- ▶ Where appropriate, specify a date according to the selection.
- ▶ Where appropriate, select the following additional options (availability depends on job type):
- **Repeat job if the time has already expired**

Past jobs are performed that could not be performed at the required time, for example because the computer was switched off.

  - ▶ Click **Next**.
    - The dialog box **Selection of the display mode** appears.
  - ▶ Select the display mode of the job window:
    - **Invisible**: No job window
    - **Minimized**: progress bar only
    - **Maximized**: Entire job window
  - ▶ Select the **Shut down computer if job is done** option if you want the computer to shut down automatically when the scan is finished. This option is only available if the display mode is set to minimized or maximized.
  - ▶ Click **Finish**.
    - Your newly created job appears on the start page of the **ADMINISTRATION > Scheduler** section with the status enabled (check mark).
  - ▶ Where appropriate, deactivate jobs that are not to be performed.

Use the following icons to further define your jobs:



View properties of a job



Edit job



Delete job



Start job





Stop job

#### 4.3.9 Targeted scan for Rootkits and active malware

To scan for active rootkits, use the predefined scan profile **Scan for Rootkits and active malware**.

To scan for active rootkits systematically:

- ▶ Go to Control Center and select the section *PC PROTECTION* > **System Scanner**.
  - Predefined scan profiles appear.
- ▶ Select the predefined scan profile **Scan for Rootkits and active malware**.
- ▶ Where appropriate, highlight other nodes and directories to be scanned by clicking the check box of the directory level.
- ▶ Click the icon (Windows XP:  or as of Windows Vista:  ).
  - The **Luke Filewalker** window appears and a system scan is started.
  - When the scan is completed, the results are displayed.

#### 4.3.10 React to detected viruses and malware

For the individual protection components of your Avira product, you can define how your Avira product reacts to a detected virus or unwanted program in the **Configuration** under the section **Action on detection**.

No configurable action options are available for the ProActiv component of the Real-Time Protection: Notification of a detection is always given in the **Real-Time Protection: Suspicious application behavior** window.

#### Action options for the System Scanner:

##### Interactive

In interactive action mode, the results of the System Scanner scan are displayed in a dialog box. This option is enabled as the default setting.

In the case of **System Scanner scan**, you will receive an alert with a list of the affected files when the scan is complete. You can use the content-sensitive menu to select an action to be executed for the various infected files. You can execute the standard actions for all infected files or cancel the System Scanner.

## Automatic

In automatic action mode, when a virus or unwanted program is detected the action you selected in this area is executed automatically.

### Action options for the Real-Time Protection:

## Interactive

In interactive action mode, data access is denied and a desktop notification is displayed. In the desktop notification you can remove the malware detected or transfer the malware to the System Scanner component using the **Details** button for further virus management. The System Scanner opens a window containing notification of the detection, which gives you various options for managing the affected file via a context menu (see Detection > System Scanner):

## Automatic

In automatic action mode, when a virus or unwanted program is detected, the action you selected in this area is executed automatically.

### Action options for Mail Protection, Web Protection:

## Interactive

In interactive action mode, if a virus or unwanted program is detected, a dialog box appears in which you can select what to do with the infected object. This option is enabled as the default setting.

## Automatic

In automatic action mode, when a virus or unwanted program is detected the action you selected in this area is executed automatically.

In interactive action mode, you can react to detected viruses and unwanted programs by selecting an action for the infected object in the alert and executing the selected action by clicking **Confirm**.

The following actions for handling infected objects are available for selection:

### Note

Which actions are available for selection depends on the operating system, the protection components (Avira Real-Time Protection, Avira System Scanner, Avira Mail Protection, Avira Web Protection) reporting the detection, and the type of malware detected.

**Actions of the System Scanner and the Real-Time Protection (not ProActiv detections):****Repair**

The file is repaired.

This option is only available if the infected file can be repaired.

**Rename**

The file is renamed with a \*.vir extension. Direct access to these files (e.g. with double-click) is therefore no longer possible. Files can be repaired and given their original name at a later time.

**Quarantine**

The file is packaged into a special format (\*.qua) and moved to the Quarantine directory *INFECTED* on your hard disk, so that direct access is no longer possible. Files in this directory can be repaired in Quarantine at a later date or, if necessary, sent to Avira.

**Delete**

The file will be deleted. This process is much quicker than **Overwrite and delete**. If a boot sector virus is detected, this can be deleted by deleting the boot sector. A new boot sector is written.

**Ignore**

No further action is taken. The infected file remains active on your computer.

**Overwrite and delete**

The file is overwritten with a default template and then deleted. It cannot be restored.

**Warning**

This could result in loss of data and damage to the operating system! Only select the **Ignore** option in exceptional cases.

**Always ignore**

Action option for Real-Time Protection detections: No further action is taken by Real-Time Protection. Access to the file is permitted. All further access to this file is permitted and no further notifications will be provided until the computer is restarted or the virus definition file is updated.

**Copy to quarantine**

Action option for a rootkits detection: The detection is copied to quarantine.

## Repair boot sector | Download repair tool

Action options when infected boot sectors are detected: A number of options are available for repairing infected diskette drives. If your Avira product is unable to perform the repair, you can download a special tool for detecting and removing boot sector viruses.

### Note

If you carry out actions on running processes, the processes in question are terminated before the actions are performed.

## Actions of the Real-Time Protection for detections made by the ProActiv component (notification of suspicious actions of an application):

### Trusted program

The application continues to run. The program is added to the list of permitted applications and is excluded from monitoring by the ProActiv component. When adding to the list of permitted applications, the monitoring type is set to *Content*. This means that the application is only excluded from monitoring by the ProActiv component if the content remains unchanged (see [Application filter: Applications to be skipped](#)).

### Block program once

The application is blocked, i.e. the application is terminated. The actions of the application continue to be monitored by the ProActiv component.

### Always block this program

The application is blocked, i.e. the application is terminated. The program is added to list of blocked applications and can no longer be run (see [Application filter: Applications to be blocked](#)).

### Ignore

The application continues to run. The actions of the application continue to be monitored by the ProActiv component.

## Mail Protection actions: Incoming emails

### Move to quarantine

The email including all attachments is moved to quarantine. The affected email is deleted. The body of the text and any attachments of the email are replaced by a [default text](#).

### Delete mail

The affected email is deleted. The body of the text and any attachments of the email are replaced by a [default text](#).

### Delete attachment

The infected attachment is replaced by a [default text](#). If the body of the email is affected, it is deleted and also replaced by a [default text](#). The email itself is delivered.

### Move attachment to quarantine

The infected attachment is placed in quarantine and then deleted (replaced by a [default text](#)). The body of the email is delivered. The affected attachment can later be delivered via the quarantine manager.

### Ignore

The affected email is delivered.

#### Warning

This could allow viruses and unwanted programs to access your computer system. Only select the **Ignore** option in exceptional cases. Disable the preview in your mail client, never open any attachments with a double click!

### Mail Protection actions: Outgoing emails

#### Move mail to quarantine (do not send)

The email, together with all attachments, is copied to Quarantine and is not sent. The email remains in the outbox of your email client. You receive an error message in your email program. All other emails sent from your email account will be scanned for malware.

#### Block sending of mails (do not send)

The email is not sent and remains in the outbox of your email client. You receive an error message in your email program. All other emails sent from your email account will be scanned for malware.

### Ignore

The affected email is sent.

#### Warning

Viruses and unwanted programs can penetrate the computer system of the email recipient in this way.

## Web Protection actions:

### Deny access

The website requested from the web server and/or any data or files transferred are not sent to your web browser. An error message to notify you that access has been denied is displayed in the web browser.

### Move to quarantine

The website requested from the web server and/or any data or files transferred are moved to quarantine. The affected file can be recovered from quarantine manager if it has an informative value or - if necessary - sent to the Avira Malware Research Center.

### Ignore

The website requested from the web server and/or the data and files that were transferred are forwarded on by Web Protection to your web browser.

#### Warning

This could allow viruses and unwanted programs to access your computer system. Only select the **Ignore** option in exceptional cases.

#### Note

We recommend that you move any suspicious file that cannot be repaired to quarantine.

#### Note

You can also send files reported by the heuristic to us for analysis. For example, you can upload these files to our website:

<http://www.avira.com/sample-upload>

You can identify files reported by the heuristic from the designation *HEUR/* or *HEURISTIC/* that prefixes the file name, e.g.: *HEUR/testfile.\**.

## 4.3.11 Handling quarantined files (\*.qua)

To handle quarantined files:


- ▶ In the Control Center, select the section *ADMINISTRATION* > **Quarantine** section.
- ▶ Check which files are involved, so that, if necessary, you can reload the original back onto your computer from another location.

If you want to see more information on a file:


- ▶ Highlight the file and click on  .
  - The dialog box **Properties** appears with more information on the file.

If you want to rescan a file:


Scanning a file is recommended if the virus definition file of your Avira product has been updated and a false positive report is suspected. This enables you to confirm a false positive with a rescan and restore the file.

- ▶ Highlight the file and click on  .
  - The file is scanned for viruses and malware using the system scan settings.
  - After the scan, the dialog **Rescan statistics** appears which displays statistics on the status of the file before and after the rescan.

To delete a file:

- ▶ Highlight the file and click on  .
- ▶ You have to confirm your choice with **Yes**.

If you want to upload the file to a Avira Malware Research Center web server for analysis:

- ▶ Highlight the file you want to upload.
- ▶ Click on  .
  - A dialog opens with a form for inputting your contact data.
- ▶ Enter all the required data.
- ▶ Select a type: **Suspicious file** or **Suspicion of false positive**.
- ▶ Select a response format: **HTML**, **Text**, **HTML & Text**.
- ▶ Click **OK**.
  - The file is uploaded to a Avira Malware Research Center web server in compressed form.

#### Note

In the following cases, analysis by the Avira Malware Research Center is recommended:

**Heuristic hits (Suspicious file):** During a scan, a file has been classified as suspicious by your Avira product and moved to quarantine: Analysis of the file by the Avira Malware Research Center has been recommended in the virus detection dialog box or in the report file generated by the scan.

**Suspicious file:** You consider a file to be suspicious and have therefore moved this file to quarantine, but a scan of the file for viruses and malware is negative.

**Suspicion of false positive:** You assume that a virus detection is a false



positive: Your Avira product reports a detection in a file, which is very unlikely to have been infected by malware.


**Note**

The size of the files you upload is limited to 20 MB uncompressed or 8 MB compressed.

**Note**

You can only upload one file at a time.

If you want to export the properties of a quarantined object to a text file:



- ▶ Highlight the quarantined object and click on  .
  - ➔ The text file *quarantaene - Notepad* opens containing the data from the selected quarantined object.
- ▶ Save the text file.

You can also restore the files in quarantine (see Chapter: [Quarantine: Restore the files in quarantine](#)).

### 4.3.12 Restore the files in quarantine



Different icons control the restore procedure, depending on the operating system:

- In Windows XP:

-  This icon restores the files to their original directory.
-  This icon restores the files to a directory of your choice.

- As of Windows Vista:

As of Microsoft Windows Vista, the Control Center only has limited rights at the moment, e.g. for access to directories and files. Certain actions and file accesses can only be performed in the Control Center with extended administrator rights. These extended administrator rights must be granted at the start of each scan via a scan profile.


-  This icon restores the files to a directory of your choice.
-  This icon restores the files to their original directory. If extended administrator rights are necessary to access this directory, a corresponding request appears.

**To restore files in quarantine:****Warning**

This could result in loss of data and damage to the operating system of the computer! Only use the function **Restore selected object** in exceptional cases. Only restore files that could be repaired by a new scan.

- ✓ File rescanned and repaired.
- ▶ In the Control Center, select the section *ADMINISTRATION* > **Quarantine** section.

**Note**


Emails and email attachments can only be restored using the option  if the file extension is \*.eml.

**To restore a file to its original location:**

- ▶ Highlight the file and click the icon (Windows XP:  , as of Windows Vista  ).


This option is not available for emails.

**Note**

Emails and email attachments can only be restored using the option  if the file extension is \*.eml.


- A message appears asking if you want to restore the file.
- ▶ Click **Yes**.
  - The file is restored to the directory it was in before it was moved to quarantine.

**To restore a file to a specified directory:**

- ▶ Highlight the file and click on  .
  - A message appears asking if you want to restore the file.
- ▶ Click **Yes**.
  - The Windows default window *Save As* for selecting the directory appears.
- ▶ Select the directory to restore the file to and confirm.
  - The file is restored to the selected directory.

### 4.3.13 Move suspicious files to quarantine

To move a suspect file to quarantine manually:

- ▶ In the Control Center, select the section *ADMINISTRATION* > **Quarantine** section.
- ▶ Click on  .
  - The Windows default window for selecting a file appears.
- ▶ Select the file and confirm with **Open**.
  - The file is moved to quarantine.

You can scan files in quarantine with the Avira System Scanner (see Chapter: [Quarantine: Handling quarantined files \(\\*.qua\)](#)).

### 4.3.14 Amend or delete file type in a scan profile

To stipulate additional file types to be scanned or exclude specific file types from the scan in a scan profile (only possible for manual selection and customized scan profiles):

- ✓ In the Control Center, go to the *PC PROTECTION* > **System Scanner** section.
- ▶ With the right-hand mouse button, click on the scan profile you want to edit.
  - A context menu appears.
- ▶ Select **File filter**.
- ▶ Expand the context menu further by clicking on the small triangle on the right-hand side of the context menu.
  - The entries **Default**, **Scan all files** and **User-defined** appear.
- ▶ Select **User-defined**.
  - The **File extensions** dialog box appears with a list of all file types to be scanned with the scan profile.

If you want to exclude a file type from the scan:

- ▶ Highlight the file type and click **Delete**.

If you want to add a file type to the scan:


- ▶ Highlight a file type.
- ▶ Click **Insert** and enter the file extension of file type into the input box.

Use a maximum of 10 characters and do not enter the leading dot. Wildcards (\* and ?) are allowed.

### 4.3.15 Create desktop shortcut for scan profile

You can start a system scan directly from your desktop via a desktop shortcut to a scan profile without accessing your Avira product's Control Center.

To create a desktop shortcut to the scan profile:

- ✓ In the Control Center, go to the *PC PROTECTION* > **System Scanner** section.
- ▶ Select the scan profile for which you want to create a shortcut.
- ▶ Click the icon  .
  - The desktop shortcut is created.

### 4.3.16 Filter events

Events that have been generated by program components of your Avira product are displayed in the Control Center under *ADMINISTRATION* > **Events** (analogous to the event display of your Windows operating system). The program components, in alphabetical order, are the following:

- Helper Service
- Mail Protection
- Real-Time Protection
- Scheduler
- System Scanner
- Updater
- Web Protection
- ProActiv

The following event types are displayed:

- *Information*
- *Warning*
- *Error*
- *Detection*

To filter displayed events:

- ▶ In the Control Center, select the section *ADMINISTRATION* > **Events**.
  - ▶ Check the box of the program components to display the events of the activated components.
- OR -

Uncheck the box of the program components to hide the events of the deactivated components.

- ▶ Check the event type box to display these events.

- OR -

Uncheck the event type box to hide these events.

#### 4.3.17 Exclude email addresses from scan


To define which email addresses (senders) are excluded from the Mail Protection scan (white listing):

- ▶ Go to Control Center and select the section *INTERNET PROTECTION* > **Mail Protection**.

→ The list shows incoming emails.

- ▶ Highlight the email you want to exclude from the Mail Protection scan.

- ▶ Click the icon to exclude the email from the Mail Protection scan:

-  The selected email address will no longer be scanned for viruses and unwanted programs.

→ The email sender address is included in the exclusion list and no longer scanned for viruses, malware .

#### **Warning**

Only exclude email addresses from the Mail Protection scan if the senders are completely trustworthy.

#### **Note**

In the Configuration, under [Mail Protection > General > Exceptions](#), you can add other email addresses to the exclusion list or remove email addresses from the exclusion list.

## 5. System Scanner

With the System Scanner component, you can carry out targeted scans (on-demand scans) for viruses and unwanted programs. The following options are available for scanning for infected files:

- **System scan via context menu**

The system scan via the context menu (right-hand mouse button - entry **Scan selected files with Avira**) is recommended if, for example, you wish to scan individual files and directories. Another advantage is that it is not necessary to first start the Control Center for a system scan via the context menu.

- **System scan via drag & drop**

When a file or directory is dragged into the program window of the Control Center, the System Scanner scans the file or directory and all sub-directories it contains. This procedure is recommended if you wish to scan individual files and directories that you have saved, for example, on your desktop.

- **System scan via profiles**

This procedure is recommended if you wish to regularly scan certain directories and drives (e.g. your work directory or drives on which you regularly store new files). You do not then need to select these directories and drives again for every new scan, you simply select using the relevant profile.

- **System scan via the Scheduler**

The Scheduler enables you to carry out time-controlled scans.

Special processes are required when scanning for rootkits, boot sector viruses, and when scanning active processes. The following options are available:

- Scan for rootkits via the scan profile **Scan for Rootkits and active malware**
- Scan active processes via the scan profile **Active processes**
- Scan for boot sector viruses via the menu command **Boot records scan...** in the menu **Extras**

## 6. Updates

The effectiveness of anti-virus software depends on how up-to-date the program is, in particular the virus definition file and the scan engine. To carry out regular updates, the Updater component is integrated into your Avira product. The Updater ensures that your Avira product is always up-to-date and able to deal with the new viruses that appear every day. Updater updates the following components:

- Virus definition file:  
The virus definition file contains the virus patterns of the harmful programs which are used by your Avira product to scan for viruses and malware and repair infected objects.
- Scan engine:  
The scan engine contains the methods used by your Avira product to scan for viruses and malware.
- Program files (product update):  
Update packages for product updates make extra functions available to the individual program components.

An update checks whether the virus definition file, the scan engine and the product are up-to-date and if necessary, implements an update. After a product update, you may have to restart your computer system. If only the virus definition file and scan engine are updated, the computer does not have to be restarted.

When a product update requires a reboot, you can decide whether to continue with the update or to be reminded again later about the update. If you continue with the product update immediately, you are still able to choose when the reboot should take place.

If you want to be reminded about the update later on, the virus definition file and the scan engine will be updated anyway, but the product update will not be done.

### Note

The product update will not be completed until a reboot has occurred.

### Note

For security reasons, the Updater checks whether the Windows *hosts* file of your computer was altered, whether the Update URL, for example, was manipulated by malware and is diverting the Updater to unwanted download sites. If the Windows *hosts* file has been manipulated, this is shown in the Updater report file.

An update is automatically performed in the following interval: 2 hours.

In the Control Center under **Scheduler**, you can create additional update jobs that are performed by Updater at the specified intervals. You also have the option to start an update manually:

- in the Control Center: in the **Update** menu and in the **Status** section
- via the context menu of the tray icon

Updates can be obtained from the Internet via Web server of the manufacturer. The existing network connection is the default connection to the download servers of Avira. You can change this default setting under [Configuration > Update](#).



## 7. FireWall

Avira Antivirus Suite allows you to manage the incoming and outgoing data traffic depending on computer settings:

- Windows Firewall

Starting from Windows 7, Avira Antivirus Suite allows the Windows Firewall management through the Avira product.

## 8. FAQ, Tips

This chapter contains important information on troubleshooting and further tips on using your Avira product.

- see Chapter [Help in case of a problem](#)
- see Chapter [Shortcuts](#)
- see Chapter [Windows Security Center](#) (Windows XP) or [Windows Action Center](#) (as of Windows 7)

### 8.1 Help in case of a problem

Here you will find information on causes and solutions of possible problems.

- The error message *The license file cannot be opened* appears.
- The error message *Connection failed while downloading the file ...* appears when attempting to start an update.
- Viruses and malware cannot be moved or deleted.
- The status of the tray icon is disabled.
- The computer is extremely slow when I perform a data back-up.
- My firewall reports Avira Real-Time Protection and Avira Mail Protection immediately after activation.
- Avira Mail Protection does not work.
- An email sent via a TLS connection has been blocked by Mail Protection.
- Webchat is not operational: Chat messages will not be displayed; data are being loaded in the browser

#### **The error message *The license file cannot be opened* appears.**

Reason: The file is encrypted.

- ▶ To activate the license, you do not need to open the file, but rather you save it in the program directory.

#### **The error message *Connection failed while downloading the file ...* appears when attempting to start an update.**

Reason: Your Internet connection is inactive. No connection to the web server on the Internet can therefore be established.

- ▶ Test whether other Internet services such as WWW or email work. If not, re-establish the Internet connection.

Reason: The proxy server cannot be reached.

- ▶ Check whether the login for the proxy server has changed and adapt it to your configuration if necessary.

Reason: The *update.exe* file is not fully approved by your personal firewall.

- ▶ Ensure that the *update.exe* file is fully approved by your personal firewall.

Otherwise:

- ▶ Check your settings in the Configuration under [PC Protection > Update](#).

### **Viruses and malware cannot be moved or deleted.**

Reason: The file was loaded by windows and is active.

- ▶ Update your Avira product.
- ▶ If you use the Windows XP operating system, deactivate System Restore.
- ▶ Start the computer in Safe Mode.
- ▶ Start the Configuration of your Avira product .
- ▶ Select [System Scanner > Scan > Files > All files](#) and confirm the window with **OK**.
- ▶ Start a scan of all local drives.
- ▶ Start the computer in Normal Mode.
- ▶ Carry out a scan in Normal Mode.
- ▶ If no other viruses or malware have been found, activate System Restore if it is available and to be used.

### **The status of the tray icon is disabled.**

Reason: Avira Real-Time Protection is disabled.

- ▶ In the Control Center click **Status** and enable the **Real-Time Protection** in the *PC Protection* area .

-OR-

- ▶ Open the context menu with a right-click on the Tray Icon. Click **Real-Time Protection enable**.

Reason: Avira Real-Time Protection is blocked by a firewall.

- ▶ Define a general approval for Avira Real-Time Protection in the configuration of your firewall. Avira Real-Time Protection only works with the address 127.0.0.1 (localhost). An Internet connection is not established. The same applies to Avira Mail Protection.

Otherwise:

- ▶ Check the startup type of the Avira Real-Time Protection service. If necessary, enable the service: In the taskbar, select **Start > Settings > Control Panel**. Start the configuration panel **Services** with a double-click (under Windows XP the services applet is located in the sub-directory *Administrative Tools*). Find the entry *Avira Real-Time Protection*. *Automatic* must be entered as the startup type and *Started* as the status. If necessary, start the service manually by selecting the relevant line and the button **Start**. If an error message appears, please check the event display.

### **The computer is extremely slow when I perform a data back-up.**

Reason: During the backup procedure, Avira Real-Time Protection scans all files being used by the backup procedure.

- ▶ Select **Real-Time Protection > Scan > Exceptions** in the Configuration and enter the process names of the back-up software.

### **My firewall reports Avira Real-Time Protection and Avira Mail Protection immediately after activation.**

Reason: Communication with Avira Real-Time Protection and Avira Mail Protection occurs via the TCP/IP Internet protocol. A firewall monitors all connections via this protocol.

- ▶ Define a general approval for Avira Real-Time Protection and Avira Mail Protection. Avira Real-Time Protection only works with the address 127.0.0.1 (localhost). An Internet connection is not established. The same applies to Avira Mail Protection.

### **Avira Mail Protection does not work.**

Please check correct functioning of Avira Mail Protection with the aid of the following checklists if problems occur with Avira Mail Protection.

#### **Checklist**

- ▶ Check whether your mail client logs in to the server via Kerberos, APOP or RPA. These verification methods are currently not supported.
- ▶ Check whether your mail client reports to the server through SSL (also often called TLS – Transport Layer Security). Avira Mail Protection does not support SSL and therefore terminates any encrypted SSL connections. If you want to use encrypted SSL connections without having them protected by Mail Protection, you will have to use a port that is not monitored by Mail Protection for the connection. The ports monitored by Mail Protection can be configured in the configuration under **Mail Protection > Scan**.
- ▶ Is the Avira Mail Protection service active? If necessary, enable the service: In the taskbar, select **Start > Settings > Control Panel**. Start the configuration panel **Services** with a double-click (under Windows XP the services applet is located in the sub-directory *Administrative Tools*). Find the entry *Avira Mail Protection*. *Automatic* must be entered as the startup type and *Started* as the status. If necessary, start

the service manually by selecting the relevant line and the button **Start**. If an error message appears, please check the event display. If this is not successful, you may have to completely uninstall the Avira product via **Start > Settings > Control Panel > Add or Remove Programs**, to restart the computer and then to reinstall your Avira product.

## General

POP3 connections encrypted via SSL (Secure Sockets Layer, also frequently referred to as TLS (Transport Layer Security)) cannot currently be protected and are ignored.

Verification to the mail server is currently only supported via passwords. "Kerberos" and "RPA" are currently not supported.

Your Avira product does not check outgoing emails for viruses and unwanted programs.

### Note

We recommend regularly installing Microsoft updates to close any gaps in security.

### **An email sent via a TLS connection has been blocked by Mail Protection.**

Reason: Transport Layer Security (TLS: encryption protocol for data transfers on the Internet) is not supported by Mail Protection at this time. The following options are available for sending the email:

- ▶ Use a port other than port 25, which is used by SMTP. This will bypass monitoring by Mail Protection.
- ▶ Turn off the TLS encrypted connection and disable TLS support in your email client.
- ▶ Disable (temporarily) the monitoring of outgoing emails by Mail Protection in the configuration under [Mail Protection > Scan](#).

### **Webchat is not operational: Chat messages will not be displayed; data are being loaded in the browser.**

This phenomenon may occur during chats, which are based on the HTTP protocol with 'transfer-encoding: chunked'.

Reason: Web Protection checks the sent data completely for viruses and undesired programs first, before the data are loaded into the web browser. During a data transfer with 'transfer-encoding: chunked', Web Protection cannot determine the message length or the data volume.

- ▶ Enter the configuration of the URL of the web chats as an exception (see Configuration: [Web Protection > Scan > Exceptions](#)).

## 8.2 Shortcuts

Keyboard commands - also called shortcuts - offer a fast possibility to navigate through the program, to retrieve individual modules and to start actions.

Below we provide you with an overview of the available keyboard commands. Please find further indications regarding the functionality in the corresponding chapter of the help.

### 8.2.1 In dialog boxes

Shortcut	Description
<b>Ctrl + Tab</b> <b>Ctrl + Page down</b>	Navigation in the Control Center Go to next section.
<b>Ctrl + Shift + Tab</b> <b>Ctrl + Page up</b>	Navigation in the Control Center Go to previous section.
← ↑ → ↓	Navigation in the configuration sections First, use the mouse to set the focus on a configuration section.  Change between the options in a marked drop-down list or between several options in a group of options.
<b>Tab</b>	Change to the next option or options group.
<b>Shift + Tab</b>	Change to the previous option or options group.
<b>Space</b>	Activate or deactivate a check box, if the active option is a check box.
<b>Alt + underlined letter</b>	Select option or start command.
<b>Alt + ↓</b> <b>F4</b>	Open selected drop-down list.

<b>Esc</b>	Close selected drop-down list. Cancel command and close dialog.
<b>Enter</b>	Start command for the active option or button.

### 8.2.2 In the help

Shortcut	Description
<b>Alt + Space</b>	Display system menu.
<b>Alt + Tab</b>	Shift between the help and the other opened windows.
<b>Alt + F4</b>	Close help.
<b>Shift + F10</b>	Display context menu of the help.
<b>Ctrl + Tab</b>	Go to next section in the navigation window.
<b>Ctrl + Shift + Tab</b>	Go to previous section in the navigation window.
<b>Page up</b>	Change to the subject, which is displayed above in the contents, in the index or in the list of the search results.
<b>Page down</b>	Change to the subject, which is displayed below the current subject in the contents, in the index or in the list of the search results.

<b>Page up</b> <b>Page down</b>	Browse through a subject.
------------------------------------	---------------------------

### 8.2.3 In the Control Center

#### General

Shortcut	Description
<b>F1</b>	Display help
<b>Alt + F4</b>	Close Control Center
<b>F5</b>	Refresh
<b>F8</b>	Open configuration
<b>F9</b>	Start update

#### Scan section

Shortcut	Description
<b>F2</b>	Rename selected profile
<b>F3</b>	Start scan with the selected profile
<b>F4</b>	Create desktop link for the selected profile
<b>Ins</b>	Create new profile



<b>Del</b>	Delete selected profile
------------	-------------------------

**Quarantine section**

Shortcut	Description
<b>F2</b>	Rescan object
<b>F3</b>	Restore object
<b>F4</b>	Send object
<b>F6</b>	Restore object to...
<b>Return</b>	Properties
<b>Ins</b>	Add file
<b>Del</b>	Delete object

**Scheduler section**

Shortcut	Description
<b>F2</b>	Edit job
<b>Return</b>	Properties
<b>Ins</b>	Insert new job
<b>Del</b>	Delete job

**Reports section**

Shortcut	Description
<b>F3</b>	Display report file
<b>F4</b>	Print report file
<b>Return</b>	Display report
<b>Del</b>	Delete report(s)

**Events section**

Shortcut	Description
<b>F3</b>	Export event(s)
<b>Return</b>	Show event
<b>Del</b>	Delete event(s)

## 8.3 Windows Security Center

- Windows XP Service Pack 2 -

### 8.3.1 General

The Windows Security Center checks the status of a computer for important security aspects.

If a problem is detected with one of these important points (e.g. an outdated anti-virus program), the Security Center issues an alert and gives recommendations on how to protect your computer better.

### 8.3.2 The Windows Security Center and your Avira product

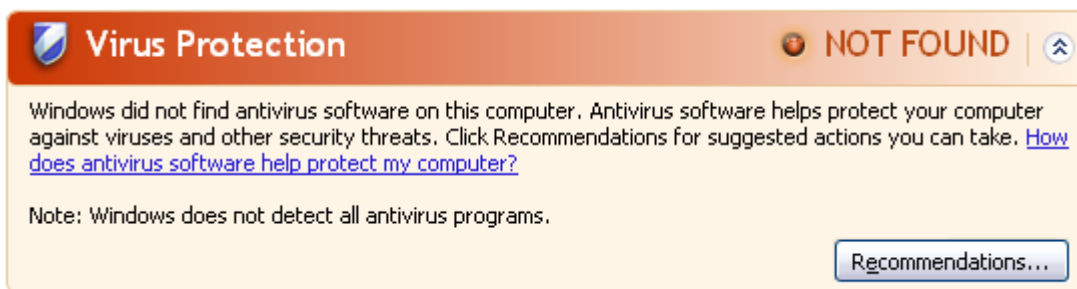
#### Virus protection software / Protection against malicious software

You may receive the following information from the Windows Security Center with regard to your virus protection:

- [Virus protection NOT FOUND](#)
- [Virus protection OUT OF DATE](#)
- [Virus protection ON](#)
- [Virus protection OFF](#)
- [Virus protection NOT MONITORED](#)

#### Virus protection NOT FOUND

This information of the Windows Security Center appears when the Windows Security Center has not found any anti-virus software on your computer.

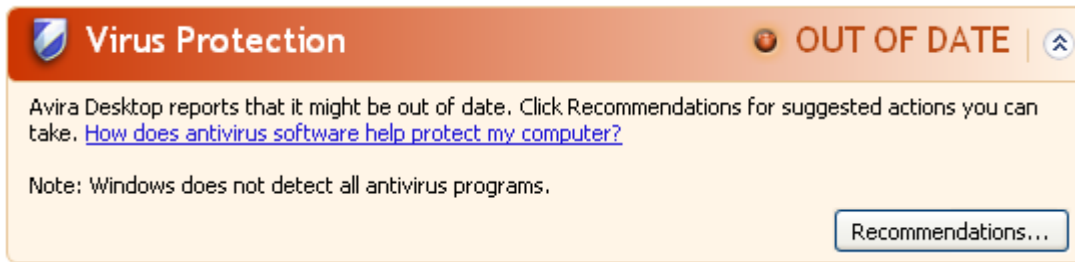


#### Note

Install your Avira product on your computer to protect it against viruses and other unwanted programs!

#### Virus protection OUT OF DATE

If you have already installed Windows XP Service Pack 2 and then install your Avira product or you install Windows XP Service Pack 2 on a system on which your Avira product has already been installed, you will receive the following message:

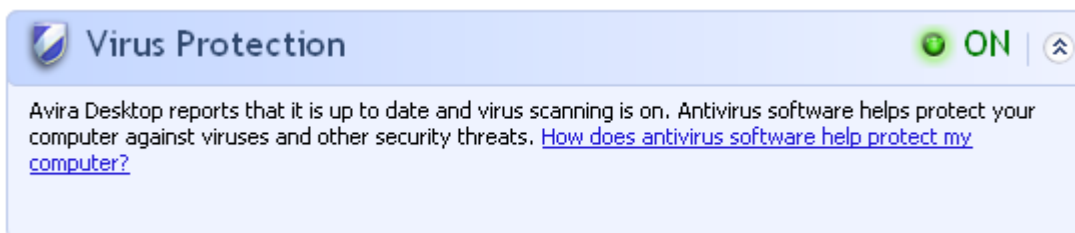


#### Note

In order for the Windows Security Center to recognize your Avira product as up-to-date, an update must be performed after installation. Update your system by carrying out an update.

### Virus protection ON

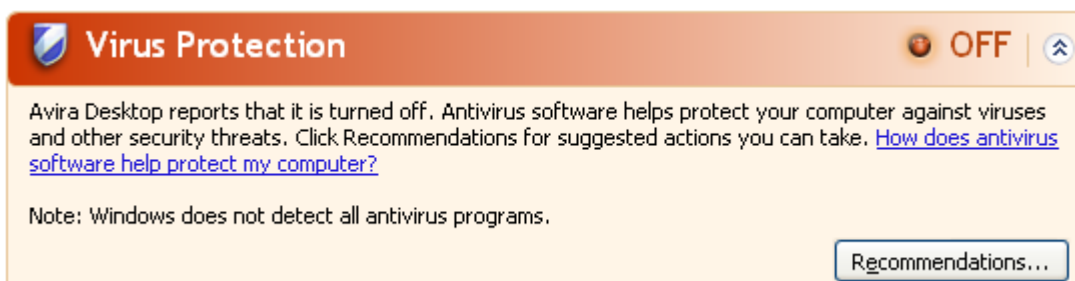
After installing your Avira product and performing a subsequent update, you will receive the following message:



Your Avira product is now up-to-date and the Avira Real-Time Protection is enabled.

### Virus protection OFF

You receive the following message if you disable the Avira Real-Time Protection or stop the Real-Time Protection service.



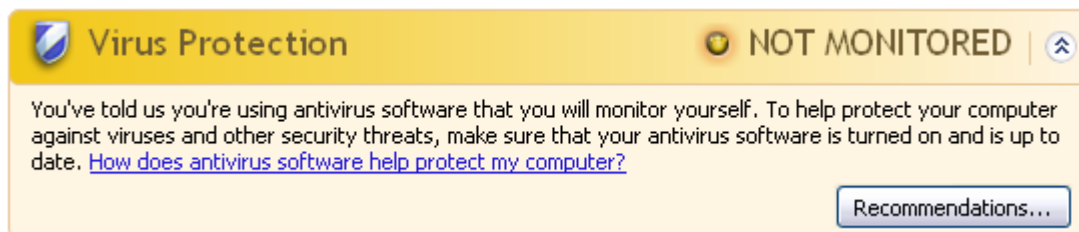
#### Note

You can enable or disable Avira Real-Time Protection in the Status section of

the **Control Center**. You can also see that the Avira Real-Time Protection is enabled if the red umbrella in your taskbar is open.

## Virus protection NOT MONITORED

If you receive the following message from the Windows Security Center, you have decided that you want to monitor your anti-virus software yourself.



### Note

The Windows Security Center is supported by your Avira product. You can enable this option at any time via the **Recommendations** button.

### Note

Even if you have installed Windows XP Service Pack 2, you still require a virus protection solution. Although Windows monitors your anti-virus software, it does not contain any anti-virus functions itself. Therefore you would not be protected against viruses and other malware without an additional anti-virus solution!

## 8.4 Windows Action Center

- Windows 7 and Windows 8 -

### 8.4.1 General

#### Note:

Starting from Windows 7 the **Windows Security Center** has been renamed to **Windows Action Center**. Under this section you will find the status of all your security options.

The Windows Action Center checks the status of a computer for important security aspects. You can access it directly by clicking the little flag in your taskbar or under **Control Panel > Action Center**.

If a problem is detected with one of these important points (e.g. an outdated anti-virus program), the Action Center issues an alert and gives recommendations on how to protect your computer better. This means, that if everything works correctly, you won't be bothered with messages. You still can have a look at the security status of your computer in the **Windows Action Center**, under the **Security** item.

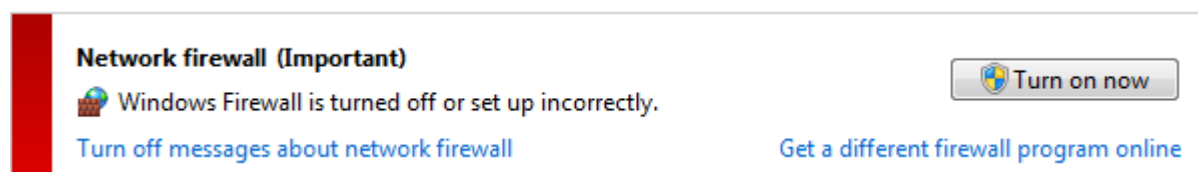
The **Windows Action Center** also gives you the option of managing the installed programs and to choose between them (e.g. *View installed antispware programs*).

You can even turn off the warning messages under **Change Action Center settings** (e.g. *Turn off messages about spyware and related protection*).

## 8.4.2 The Windows Action Center and your Avira product

- [Windows Firewall is turned off or set up incorrectly](#)

### Windows Firewall is turned off or set up incorrectly



- **Avira-managed Windows Firewall installed**
- Starting from Windows 7, Avira Antivirus Suite gives you the option of managing directly the Windows Firewall from the Avira Control and Configuration Center.

### Virus protection

You may receive the following information from the Windows Action Center with regard to your virus protection:

- [Avira Desktop reports that it is up to date and virus scanning is on.](#)
- [Avira Desktop reports that it is turned off.](#)
- [Avira Desktop reports that it is out of date.](#)
- [Windows did not find antivirus software on this computer.](#)
- [Avira Desktop has expired.](#)

### Avira Desktop reports that it is up to date and virus scanning is on

After installation of your Avira product and a subsequent update, you will not receive any messages from the Windows Action Center. But if you go to **Action Center > Security** you can see: *Avira Desktop reports that it is up to date and virus scanning is on.* This means that your Avira product is now up-to-date and the Avira Real-Time Protection is enabled.

## Avira Desktop reports that it is turned off

You receive the following message if you disable the Avira Real-Time Protection or stop the Real-Time Protection service.

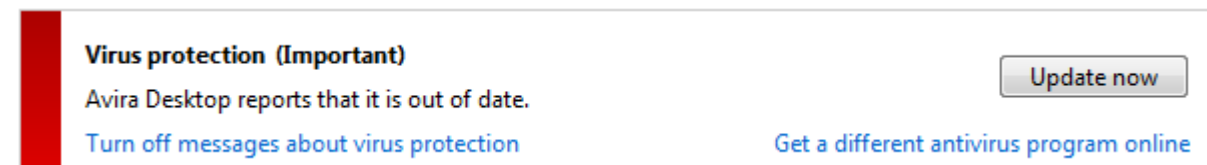


### Note

You can enable or disable Avira Real-Time Protection in the **Status** section of the **Avira Control Center**. You can also notice that the Avira Real-Time Protection is enabled by the opened red umbrella in your taskbar. It is also possible to activate the Avira product by clicking the *Turn on now* button on the Windows Action Center message. You will receive a notification asking your permission to run Avira. Click on *Yes, I trust the publisher and want to run this program* and Real-Time Protection will be enabled again.

## Avira Desktop reports that it is out of date

If you just installed Avira or if for some reason the virus definition file, the scan engine or the program files of your Avira product have not been updated automatically (e.g. if you have made an upgrade from an older Windows operating system, on which your Avira product is already installed), you will receive the following message:



### Note

In order for the Windows Action Center to recognize your Avira product as up-to-date, an update must be performed after installation. Update your Avira Product by carrying out an update.

## Windows did not find antivirus software on this computer

This information of the Windows Action Center appears, when the Windows Action Center has not found any anti-virus software on your computer.

**Virus protection (Important)**

Windows did not find antivirus software on this computer.

[Find a program online](#)[Turn off messages about virus protection](#)**Note**

Please note that this option will not appear in Windows 8, as Windows Defender is now also the pre-set virus protection function.

**Note**

Install your Avira product on your computer to protect it against viruses and other unwanted programs!

## Avira Desktop has expired

This information of the Windows Action Center appears when the license of your Avira product has expired.

If you click on the button **Renew subscription**, you will be redirected to the website of Avira, where you can buy a new license.

**Virus protection (Important)**

Avira Desktop has expired.

[Renew subscription](#)[Turn off messages about virus protection](#)[View installed antivirus apps](#)**Note**

Please note that this option is only available for Windows 8.

## Spyware and unwanted software protection

You may receive the following information from the Windows Action Center with regard to your spyware protection:

- [Avira Desktop reports that it is turned on.](#)
- [Windows Defender and Avira Desktop both report that they are turned off.](#)
- [Avira Desktop reports that it is out of date.](#)
- [Windows Defender is out of date.](#)
- [Windows Defender is turned off.](#)



## Avira Desktop reports that it is turned on

After the installation of your Avira product and a subsequent update, you will not receive any messages from the Windows Action Center. But if you go to **Action Center > Security**, you can see: *Avira Desktop reports that it is turned on*. This means that your Avira product is now up-to-date and the Avira Real-Time Protection is enabled.

## Windows Defender and Avira Desktop both report that they are turned off

You receive the following message if you disable the Avira Real-Time Protection or stop the Real-Time Protection service.

**Spyware and unwanted software protection (Important)**

Windows Defender and Avira Desktop both report that they are turned off.

[View antispware programs](#)

[Turn off messages about spyware and related protection](#)

### Note

You can enable or disable Avira Real-Time Protection in the **Status** section of the **Avira Control Center**. You can also notice that the Avira Real-Time Protection is enabled by the opened red umbrella in your taskbar. It is also possible to activate the Avira product by clicking the *Turn on now* button on the Windows Action Center message. You will receive a notification asking your permission to run Avira. Click on *Yes, I trust the publisher and want to run this program* and Real-Time Protection will be enabled again.

## Avira Desktop reports that it is out of date

If you just installed Avira or if for some reason the virus definition file, the scan engine or the program files of your Avira product have not been updated automatically (e.g. if you have made an upgrade from an older Windows operating system, on which your Avira product is already installed), you will receive the following message:

**Spyware and unwanted software protection (Important)**

Avira Desktop reports that it is out of date.

[Update now](#)

[Turn off messages about spyware and related protection](#)

[Get a different antispware program online](#)

### Note

In order for the Windows Action Center to recognize your Avira product as up-to-date, an update must be performed after installation. Update your Avira Product by carrying out an update.

## Windows Defender is out of date

You may receive the following message if Windows Defender is activated. If you have already installed the Avira product, this message should not appear. Please check if the installation went OK.

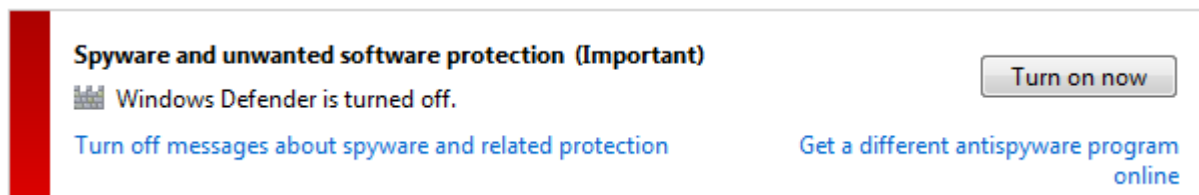


### Note

Windows Defender is the pre-set spyware and virus protection solution from Windows.

## Windows Defender is turned off

This information of the Windows Action Center appears when the Windows Action Center has not found any other anti-virus software on your computer than the one that the operating system integrates by default: Windows Defender. If you have had some anti-virus software installed on your computer before, this application has been disabled. If you have already installed the Avira product, this message should not appear: Avira should be automatically detected. Please check if the installation went OK.



## 9. Viruses and more

Avira Antivirus Suite not only detects viruses and malware, it can also protect you from other threats. In this chapter you can find an overview of different kinds of malware and other threats describing their background, behavior and the unpleasant surprises they have in store for you.

### Related topics:

- [Threat categories](#)
- [Viruses and other malware](#)

### 9.1 Threat categories

#### Adware

Adware is software that presents banner ads or in pop-up windows through a bar that appears on a computer screen. These advertisements usually cannot be removed and are consequently always visible. The connection data allow many conclusions on the usage behavior and are problematic in terms of data security.

Your Avira product detects Adware. If the **Adware** option is enabled with a check mark in the configuration under [Threat categories](#), you receive a corresponding alert if your Avira product detects adware.

#### Adware/Spyware

Software that displays advertising or software that sends the user's personal data to a third party, often without their knowledge or consent, and for this reason may be unwanted.

Your Avira product recognizes "Adware/Spyware". If the option **Adware/Spyware** is enabled with a check mark in the configuration under [Threat categories](#), you receive a corresponding alert if your Avira product detects adware or spyware.

#### Application

The term APPL, respectively application, refers to an application which may involve a risk when used or is of dubious origin.

Your Avira product recognizes "Application (APPL)". If the option **Application** is enabled with a check mark in the configuration under [Threat categories](#), you receive a corresponding alert if your Avira product detects such behavior.

## Backdoor Clients

In order to steal data or manipulate computers, a backdoor server program is smuggled in unknown to the user. This program can be controlled by a third party using backdoor control software (client) via the Internet or a network.

Your Avira product recognizes "Backdoor control software". If the **Backdoor control software** option is enabled with a check mark in the configuration under [Threat categories](#), you receive a corresponding alert if your Avira product detects such software.

## Dialer

Certain services available in the Internet have to be paid for. They are invoiced in Germany via dialers with 0190/0900 numbers (or via 09x0 numbers in Austria and Switzerland; in Germany, the number is set to change to 09x0 in the medium term). Once installed on the computer, these programs guarantee a connection via a suitable premium rate number whose scale of charges can vary widely.

The marketing of online content via your telephone bill is legal and can be of advantage to the user. Genuine dialers leave no room for doubt that they are used deliberately and intentionally by the user. They are only installed on the user's computer subject to the user's consent, which must be given via a completely unambiguous and clearly visible labeling or request. The dial-up process of genuine dialers is clearly displayed. Moreover, genuine dialers tell you the incurred costs exactly and unmistakably.

Unfortunately there are also dialers which install themselves on computers unnoticed, by dubious means or even with deceptive intent. For example they replace the Internet user's default data communication link to the ISP (Internet Service Provider) and dial a cost-incurring and often horrendously expensive 0190/0900 number every time a connection is made. The affected user will probably not notice until his next phone bill that an unwanted 0190/0900 dialer program on his computer has dialed a premium rate number with every connection, resulting in dramatically increased costs.

We recommend that you ask your telephone provider to block this number range directly for immediate protection against undesired dialers (0190/0900 dialers).

Your Avira product can detect the familiar dialers by default.

If the option **Dialers** is enabled with a check mark in the configuration under [Threat categories](#), you receive a corresponding alert if a dialer is detected. You can now simply delete the potentially unwanted 0190/0900 dialer. However, if it is a wanted dial-up program, you can declare it an exceptional file and this file is then no longer scanned in future.

## Double Extension Files

Executable files that hide their real file extension in a suspicious way. This camouflage method is often used by malware.

Your Avira product recognizes "Double Extension Files". If the option **Double Extension files** is enabled with a check mark in the configuration under [Threat categories](#), you receive a corresponding alert if your Avira product detects such files.

### **Fraudulent software**

Also known as "scareware" or "rogueware", it is a fraudulent software that pretends that your computer is infected by viruses or malware. This software looks deceptively similar to professional antivirus software but is meant to raise uncertainty or to scare the user. Its purpose is to make the victims feel threatened of imminent (unreal) danger and to make them pay to eliminate it. There are also cases when the victims are lead to believe they were attacked and they are instructed to carry out an action, which in reality is the real attack.

Your Avira product detects scareware. If the option **Fraudulent software** is enabled with a check mark in the configuration [Threat categories](#), you receive a corresponding alert if your Avira product detects such files.

### **Games**

There is a place for computer games - but it is not necessarily at work (except perhaps in the lunch hour). Nevertheless, with the wealth of games downloadable from the Internet, a fair bit of mine sweeping and Patience playing goes on among company employees and civil servants. You can download a whole array of games via the Internet. Email games have also become more popular: numerous variants are circulating, ranging from simple chess to "fleet exercises" (including torpedo combats): The corresponding moves are sent to partners via email programs, who answer them.

Studies have shown that the number of working hours devoted to computer games has long reached economically significant proportions. It is therefore not surprising that more and more companies are considering ways of banning computer games from workplace computers.

Your Avira product recognizes computer games. If the **Games** option is enabled with a check mark in the configuration under [Threat categories](#), you receive a corresponding alert if your Avira product detects a game. The game is now over in the truest sense of the word, because you can simply delete it.

### **Jokes**

Jokes are merely intended to give someone a fright or provide general amusement without causing harm or reproducing. When a joke program is loaded, the computer will usually start at some point to play a tune or display something unusual on the screen. Examples of jokes are the washing machine in the disk drive (DRAIN.COM) or the screen eater (BUGSRES.COM).

But beware! All symptoms of joke programs may also originate from a virus or Trojan. At the very least users will get quite a shock or be thrown into such a panic that they themselves may cause real damage.

Thanks to the extension of its scanning and identification routines, your Avira product is able to detect joke programs and eliminate them as unwanted programs if required. If the option **Jokes** is enabled with a check mark in the configuration under [Threat categories](#), a corresponding alert is issued if a joke program is detected.

## Phishing

Phishing, also known as "brand spoofing" is a clever form of data theft aimed at customers or potential customers of Internet service providers, banks, online banking services, registration authorities.

When submitting your email address on the Internet, filling in online forms, accessing newsgroups or websites, your data can be stolen by "Internet crawling spiders" and then used without your permission to commit fraud or other crimes.

Your Avira product recognizes "Phishing". If the option **Phishing** is enabled with a check mark in the configuration under [Threat categories](#), you receive a corresponding alert if your Avira product detects such behavior.

## Programs that violate the private domain

Software that may be able to compromise the security of your system, initiate unwanted program activities, damage your privacy or spy on your user behavior and could therefore be unwanted.

Your Avira product detects "Security Privacy Risk" software. If the option **Programs that violate the private domain** is enabled with a check mark in the configuration under [Threat categories](#), you receive a corresponding alert if your Avira product detects such software.

## Unusual Runtime Packers

Files that have been compressed with an unusual runtime packer and that can therefore be classified as potentially suspicious.

Your Avira product recognizes "Unusual runtime packers". If the option **Unusual runtime packers** is enabled with a check mark in the configuration under [Threat categories](#), you receive a corresponding alert if your Avira product detects such packers.

# 9.2 Viruses and other malware

## Adware

Adware is software that presents banner ads or in pop-up windows through a bar that appears on a computer screen. These advertisements usually cannot be removed and are consequently always visible. The connection data allow many conclusions on the usage behavior and are problematic in terms of data security.

## **Backdoors**

A backdoor can gain access to a computer by bypassing the computer access security mechanisms.

A program that is being executed in the background generally enables the attacker almost unlimited rights. User's personal data can be spied with the backdoor's help. But are mainly used to install further computer viruses or worms on the relevant system.

## **Boot viruses**

The boot or master boot sector of hard disks is mainly infected by boot sector viruses. They overwrite important information necessary for the system execution. One of the awkward consequences: the computer system cannot be loaded any more...

## **Bot-Net**

A bot-net is defined as a remote network of PCs (on the Internet) that is composed of bots that communicate with each other. A bot-net can comprise a collection of cracked machines running programs (usually referred to as worms, Trojans) under a common command and control infrastructure. Bot-nets serve various purposes, including denial-of-service attacks etc., usually without the affected PC user's knowledge. The main potential of bot-nets is that the networks can achieve grow to thousands of computers and their total bandwidth exceeds most conventional Internet accesses.

## **Exploit**

An exploit (security gap) is a computer program or script that takes advantage of a bug, glitch or vulnerability leading to privilege escalation or denial of service on a computer system. One form of exploitation for example is an attack from the Internet with the help of manipulated data packages. Programs can be infiltrated in order to obtain higher access.

## **Fraudulent software**

Also known as "scareware" or "rogueware", it is a fraudulent software that pretends that your computer is infected by viruses or malware. This software looks deceptively similar to professional Antivirus software but is meant to raise uncertainty or to scare the user. Its purpose is to make the victims feel threatened of imminent (unreal) danger and to make them pay to eliminate it. There are also cases when the victims are lead to believe they were attacked and they are instructed to carry out an action, which in reality is the real attack.



## **Hoaxes**

For several years, Internet and other network users have received alerts about viruses that are purportedly spread via email. These alerts are spread via email with the request that they should be sent to the highest possible number of colleagues and to other users, in order to warn everyone against the "danger".

## **Honeypot**

A honeypot is a service (program or server) installed in a network. Its function is to monitor a network and log attacks. This service is unknown to the legitimate user - because of this reason he is never addressed. If an attacker examines a network for the weak points and uses the services which are offered by a honeypot, it is logged and an alert is triggered.

## **Macro viruses**

Macro viruses are small programs that are written in the macro language of an application (e.g. WordBasic under WinWord 6.0) and that can normally only spread within documents of this application. Because of this, they are also called document viruses. In order to be active, they need that the corresponding applications are activated and that one of the infected macros has been executed. Unlike "normal" viruses, macro viruses consequently do not attack executable files but they do attack the documents of the corresponding host application.

## **Pharming**

Pharming is a manipulation of the host file of web browsers to divert enquiries to spoofed websites. This is a further development of classic phishing. Pharming fraudsters operate their own large server farms on which fake websites are stored. Pharming has established itself as an umbrella term for various types of DNS attacks. In the case of a manipulation of the host file, a specific manipulation of a system is carried out with the aid of a Trojan or virus. The result is that the system can now only access fake websites, even if the correct web address is entered.

## **Phishing**

Phishing means angling for personal details of the Internet user. Phishers generally send their victims apparently official letters such as emails that are intended to induce them to reveal confidential information to the culprits in good faith, in particular user names and passwords or PINs and TANs of online banking accounts. With the stolen access details, the phishers can assume the identities of the victims and carry out transactions in their name. What is clear is that: banks and insurance companies never ask for credit card numbers, PINs, TANs or other access details by email, SMS or telephone.



## **Polymorph viruses**

Polymorph viruses are the real masters of disguise. They change their own programming codes - and are therefore very hard to detect.

## **Program viruses**

A computer virus is a program that is capable of attaching itself to other programs after being executed and cause an infection. Viruses multiply themselves unlike logic bombs and Trojans. In contrast to a worm, a virus always requires a program as host, where the virus deposits its virulent code. The program execution of the host itself is not changed as a rule.

## **Rootkits**

A rootkit is a collection of software tools that are installed after a computer system has been infiltrated to conceal logins of the infiltrator, hide processes and record data - generally speaking: to make themselves invisible. They attempt to update already installed spy programs and reinstall deleted spyware.

## **Script viruses and worms**

Such viruses are extremely easy to program and they can spread - if the required technology is on hand - within a few hours via email round the globe.

Script viruses and worms use one of the script languages, such as Javascript, VBScript etc., to insert themselves in other, new scripts or to spread themselves by calling operating system functions. This frequently happens via email or through the exchange of files (documents).

A worm is a program that multiplies itself but that does not infect the host. Worms cannot consequently form part of other program sequences. Worms are often the only possibility to infiltrate any kind of damaging programs on systems with restrictive security measures.

## **Spyware**

Spyware are so called spy programs that intercept or take partial control of a computer's operation without the user's informed consent. Spyware is designed to exploit infected computers for commercial gain.

## **Trojan horses (short Trojans)**

Trojans are pretty common nowadays. Trojans include programs that pretend to have a particular function, but that show their real image after execution and carry out a different function that, in most cases, is destructive. Trojan horses cannot multiply themselves,

which differentiates them from viruses and worms. Most of them have an interesting name (SEX.EXE or STARTME.EXE) with the intention to induce the user to start the Trojan. Immediately after execution they become active and can, for example, format the hard disk. A dropper is a special form of Trojan that 'drops' viruses, i.e. embeds viruses on the computer system.

## **Zombie**

A zombie PC is a computer that is infected with malware programs and that enables hackers to abuse computers via remote control for criminal purposes. On command, the affected PC starts denial-of-service (DoS) attacks, for example, or sends spam and phishing emails.

## 10. Info and Service

This chapter contains information on how to contact us.

- see Chapter [Contact address](#)
- see Chapter [Technical support](#)
- see Chapter [Suspicious files](#)
- see Chapter [Reporting false positives](#)
- see Chapter [Your feedback for more security](#)

### 10.1 Contact address

If you have any questions or requests concerning the Avira product range, we will be pleased to help you. For our contact addresses, please refer to the Control Center under **Help > About Avira Antivirus Suite**.

### 10.2 Technical support

Avira support provides reliable assistance in answering your questions or solving a technical problem.

All necessary information on our comprehensive support service can be obtained from our website:

<http://www.avira.com/en/support>

So that we can provide you with fast, reliable help, you should have the following information ready:

- **License information.** You can find this information in the program interface under the menu item **Help > About Avira Antivirus Suite > License information**. See License information.
- **Version information.** You can find this information in the program interface under the menu item **Help > About Avira Antivirus Suite > Version information**. See Version information.
- **Operating system version** and any Service Packs installed.
- **Installed software packages**, e.g. anti-virus software of other vendors.
- **Exact messages** of the program or of the report file.

## 10.3 Suspicious files

Suspect files or viruses that may not yet be detected or removed by our products can be sent to us. We provide you with several ways of doing this.

- Identify the file in the quarantine manager of the Control Center and select the item **Send file** via the context menu or the corresponding button.
- Send the required file packed (WinZIP, PKZip, Arj, etc.) in the attachment of an email to the following address:  
[virus@avira.com](mailto:virus@avira.com)  
As some email gateways work with anti-virus software, you should also provide the file(s) with a password (please remember to tell us the password).
- You can also send us the suspicious file via our website: <http://www.avira.com/sample-upload>

## 10.4 Reporting false positives

If you believe that your Avira product is reporting a detection in a file that is most likely "clean", send the relevant file packed (WinZIP, PKZip, Arj, etc.) as an email attachment to the following address:

[virus@avira.com](mailto:virus@avira.com)

As some email gateways work with anti-virus software, you should also provide the file(s) with a password (please remember to tell us the password).

## 10.5 Your feedback for more security

At Avira, our customers' security is paramount. For this reason, we don't just have an in-house expert team that tests the quality and security of every Avira solution before the product is released. We also attach great importance to the indications regarding security relevant gaps that could develop and we treat those seriously.

If you think you have detected a security gap in one of our products, please send us an email to the following address:

[vulnerabilities@avira.com](mailto:vulnerabilities@avira.com)

## 11. Reference: Configuration options

The configuration reference documents all available configuration options.

### 11.1 System Scanner

The **System Scanner** section of configuration is responsible for the configuration of the on-demand scan.

#### 11.1.1 Scan

You can define the behavior of the on-demand scan routine. If you select certain directories to be scanned, depending on the configuration, the System Scanner scans:

- with a certain scanning priority,
- also boot sectors and main memory,
- all or selected files in the directory.

##### *Files*

The System Scanner can use a filter to scan only those files with a certain extension (type).

##### **All files**

If this option is enabled, all files are scanned for viruses or unwanted programs, irrespective of their content and file extension. The filter is not used.

##### **Note**

If **All files** is enabled, the button **File extensions** cannot be selected.

##### **Use smart extensions**

If this option is enabled, the selection of the files scanned for viruses or unwanted programs is automatically chosen by the program. This means that your Avira program decides whether the files are scanned or not based on their content. This procedure is somewhat slower than [Use file extension list](#), but more secure, since not only on the basis of the file extension is scanned. This option is enabled as the default setting and is recommended.

##### **Note**

If **Use smart extensions** is enabled, the button **File extensions** cannot be selected.

## Use file extension list

If this option is enabled, only files with a specified extension are scanned. All file types that may contain viruses and unwanted programs are preset. The list can be edited manually via the button **"File extension"**.

### Note

If this option is enabled and you have deleted all entries from the list with file extensions, this is indicated with the text *"No file extensions"* under the button **File extensions**.

## File extensions

With the aid of this button, a dialog box is opened in which all file extensions are displayed that are scanned in **"Use file extension list"** mode. Default entries are set for the extensions, but entries can be added or deleted.

### Note

Please note that the default list may vary from version to version.

## Additional settings

### Scan boot sectors of selected drives

If this option is enabled, the System Scanner scans the boot sectors of the drives selected for the system scan. This option is enabled as the default setting.

### Scan master boot sectors

If this option is enabled, the System Scanner scans the master boot sectors of the hard disk(s) used in the system.

### Ignore offline files

If this option is enabled, the direct scan ignores so-called offline files completely during a scan. This means that these files are not scanned for viruses and unwanted programs. Offline files are files that were physically moved by a so-called Hierarchical Storage Management System (HSMS) from the hard disk onto a tape, for example. This option is enabled as the default setting.

### Integrity checking of system files

When this option is enabled, the most important Windows system files are subjected to a particularly secure check for changes by malware during every on-demand scan. If an amended file is detected, this is reported as suspect. This function uses a lot of computer capacity. That is why the option is disabled as the default setting.

**Note**

This option is only available with Windows Vista and higher.

**Note**

This option should not be used if you are using third-party tools that modify system files and adapt the boot or start screen to your own requirements. Examples of such tools are skinpacks, TuneUp utilities or Vista Customization.

**Optimized scan**

When the option is enabled, the processor capacity is optimally utilized during a System Scanner scan. For performance reasons, an optimized scan is only logged on standard level.

**Note**

This option is only available on multi-processor systems.

**Follow symbolic links**

If this option is enabled, System Scanner performs a scan that follows all symbolic links in the scan profile or selected directory and scans the linked files for viruses and malware.

**Note**

The option does not include any shortcuts, but refers exclusively to symbolic links (generated by mklink.exe) or Junction Points (generated by junction.exe) that are transparent in the file system.

**Search for Rootkits before scan**

If this option is enabled and a scan is started, the System Scanner scans the Windows system directory for active rootkits in a so-called shortcut. This process does not scan your computer for active rootkits as comprehensively as the scan profile "**Scan for rootkits**", but it is significantly quicker to perform. This option only changes the settings of profiles created by you.

**Note**

The rootkits scan is not available for Windows XP 64 bit

## Scan Registry

If this option is enabled, the Registry is scanned for references to malware. This option only changes the settings of profiles created by you.

## Ignore files and paths on network drives

If this option is enabled, network drives connected to the computer are excluded from the on-demand scan. This option is recommended when the servers or other workstations are themselves protected with anti-virus software. This option is disabled as the default setting.

## Scan process

### Allow stopping the Scanner

If this option is enabled, the scan for viruses or unwanted programs can be terminated at any time with the button **"Stop"** in the "Luke Filewalker" window. If you have disabled this setting, the **Stop** button in the "Luke Filewalker" window has a gray background. Premature ending of a scan process is thus not possible! This option is enabled as the default setting.

## Scanner priority

With the on-demand scan, the System Scanner distinguishes between priority levels. This is only effective if several processes are running simultaneously on the workstation. The selection affects the scanning speed.

### low

The System Scanner is only allocated processor time by the operating system, if no other process requires computation time, i.e. as long as only the System Scanner is running, the speed is maximum. All in all, work with other programs is optimal: The computer responds more quickly if other programs require computation time while the System Scanner continues running in the background.

### medium

The System Scanner is executed with normal priority. All processes are allocated the same amount of processor time by the operating system. This option is enabled as the default setting and is recommended. Under certain circumstances, work with other applications may be affected.

### high

The System Scanner has the highest priority. Simultaneous work with other applications is almost impossible. However, the System Scanner completes its scan at maximum speed.

## Action on detection

You can define the actions to be performed by System Scanner when a virus or unwanted program is detected.



## Interactive

If this option is enabled, the results of the System Scanner scan are displayed in a dialog box. When carrying out a scan with the System Scanner, you will receive an alert with a list of the affected files at the end of the scan. You can use the content-sensitive menu to select an action to be executed for the various infected files. You can execute the standard actions for all infected files or cancel the System Scanner.

### Note

The action **Quarantine** is preselected by default in the System Scanner notification. Further actions can be selected via a context menu.

## Automatic

If this option is enabled, no dialog box in case of a virus detection appears. The System Scanner reacts according to the settings you predefine in this section as primary and secondary action.

### Copy file to quarantine before action

If this option is enabled, the System Scanner creates a backup copy before carrying out the requested primary or secondary action. The back-up copy is saved in Quarantine, where the file can be restored if it is of informative value. You can also send the backup copy to the Avira Malware Research Center for further investigation.

### *Primary action*

Primary action is the action performed when the System Scanner finds a virus or an unwanted program. If the option "**Repair**" is selected but the affected file cannot be repaired, the action selected under "**Secondary action**" is performed.

### Note

The option **Secondary action** can only be selected if the setting **Repair** was selected under **Primary action**.

## Repair

If this option is enabled, the System Scanner repairs affected files automatically. If the System Scanner cannot repair an affected file, it carries out the action selected under **Secondary action**.

### Note

An automatic repair is recommended, but means that the System Scanner modifies files on the workstation.

**Rename**

If this option is enabled, the System Scanner renames the file. Direct access to these files (e.g. with double-click) is therefore no longer possible. Files can later be repaired and given their original names again.

**Quarantine**

If this option is enabled, the System Scanner moves the file to the quarantine. These files can later be repaired or - if necessary - sent to the Avira Malware Research Center.

**Delete**

If this option is enabled, the file is deleted. This process is much faster than "overwrite and delete".

**Ignore**

If this option is enabled, access to the file is allowed and the file is left as it is.

**Warning**

The affected file remains active on your workstation! It may cause serious damage on your workstation!

**Overwrite and delete**

If this option is enabled, the System Scanner overwrites the file with a default pattern and then deletes it. It cannot be restored.

*Secondary action*

The option "**Secondary action**" can only be selected if the setting **Repair** was selected under "**Primary action**". With this option it can now be decided what is to be done with the affected file if it cannot be repaired.

**Rename**

If this option is enabled, the System Scanner renames the file. Direct access to these files (e.g. with double-click) is therefore no longer possible. Files can later be repaired and given their original names again.

**Quarantine**

If this option is enabled, the System Scanner moves the file to Quarantine. These files can later be repaired or - if necessary - sent to the Avira Malware Research Center.

**Delete**

If this option is enabled, the file is deleted. This process is much faster than "overwrite and delete".

**Ignore**

If this option is enabled, access to the file is allowed and the file is left as it is.

**Warning**

The affected file remains active on your workstation! It may cause serious damage on your workstation!

**Overwrite and delete**

If this option is enabled, the System Scanner overwrites the file with a default pattern and then deletes (wipes) it. It cannot be restored.

**Note**

If you have selected **Delete** or **Overwrite and delete** as the primary or secondary action, you should note the following: In the case of heuristic hits, the affected files are not deleted, but are instead moved to quarantine.

**Archives**

When scanning archives, the System Scanner uses a recursive scan: Archives in archives are also unpacked and scanned for viruses and unwanted programs. The files are scanned, decompressed and scanned again.

**Scan archives**

If this option is enabled, the selected archives in the archive list are scanned. This option is enabled as the default setting.

**All archive types**

If this option is enabled, all archive types in the archive list are selected and scanned.

**Smart Extensions**

If this option is enabled, the System Scanner detects whether a file is a packed file format (archive), even if the file extension differs from the usual extensions, and scans the archive. However every file must be opened for this, which reduces the scanning speed. Example: If a \*.zip archive has the file extension \*.xyz, the System Scanner also unpacks this archive and scans it. This option is enabled as the default setting.

**Note**

Only those archive types marked in the archive list are supported.

**Limit recursion depth**

Unpacking and scanning recursive archives can require a great deal of computer time and resources. If this option is enabled, you limit the depth of the scan in multi-packed archives to a certain number of packing levels (maximum recursion depth). This saves time and computer resources.

**Note**

In order to find a virus or an unwanted program in an archive, the System Scanner must scan up to the recursion level in which the virus or the unwanted program is located.

**Maximum recursion depth**

In order to enter the maximum recursion depth, the option [Limit recursion depth](#) must be enabled.

You can either enter the requested recursion depth directly or by means of the right arrow key on the entry field. The permitted values are 1 to 99. The standard value is 20 which is recommended.

**Default values**

The button restores the pre-defined values for scanning archives.

**Archives**

In this display area you can set which archives the System Scanner should scan. For this, you must select the relevant entries.

**Exceptions***File objects to be omitted for the System Scanner*

The list in this window contains files and paths that should not be included by the System Scanner in the scan for viruses or unwanted programs.

Please enter as few exceptions as possible here and really only files that, for whatever reason, should not be included in a normal scan. We recommend that you always scan these files for viruses or unwanted programs before they are included in this list!

**Note**

The entries in the list must not result in more than 6000 characters in total.

**Warning**

These files are not included in a scan!

**Note**

The files included in this list are recorded in the [report file](#). Please check the report file from time to time for unscanned files, as perhaps the reason you excluded a file here no longer exists. In this case you should remove the name of this file from this list again.

## Input box

In this input box you can enter the name of the file object that is not included in the on-demand scan. No file object is entered as the default setting.



The button opens a window in which you can select the required file or the required path.

When you have entered a file name with its complete path, only this file is not scanned for infection. If you have entered a file name without a path, all files with this name (irrespective of the path or drive) are not scanned.

## Add

With this button, you can add the file object entered in the input box to the display window.

## Delete

The button deletes a selected entry from the list. This button is inactive if no entry is selected.

## Heuristic

This configuration section contains the settings for the heuristic of the scan engine.

Avira products contain very powerful heuristics that can proactively uncover unknown malware, i.e. before a special virus signature to combat the damaging element has been created and before a virus guard update has been sent. Virus detection involves an extensive analysis and investigation of the affected codes for functions typical of malware. If the code being scanned exhibits these characteristic features, it is reported as being suspicious. This does not necessarily mean that the code is in fact malware. False positives do sometimes occur. The decision on how to handle affected code is to be made by the user, e.g. based on his or her knowledge of whether the source of the code is trustworthy or not.

### *Macrovirus heuristic*

#### **Macrovirus heuristic**

Your Avira product contains a highly powerful macrovirus heuristic. If this option is enabled, all macros in the relevant document are deleted in the event of a repair, alternatively suspect documents are only reported, i.e. you receive an alert. This option is enabled as the default setting and is recommended.

### *Advanced Heuristic Analysis and Detection (AHeAD)*

## Enable AHeAD

Your Avira program contains a very powerful heuristic in the form of Avira AHeAD technology, which can also detect unknown (new) malware. If this option is enabled, you can define how "aggressive" this heuristic should be. This option is enabled as the default setting.

### Low detection level

If this option is enabled, slightly less unknown malware is detected, the risk of false alerts is low in this case.

### Medium detection level

This option combines a strong detection level with a low risk of false alerts. Medium is the default setting if you have selected the use of this heuristic.

### High detection level

If this option is enabled, significantly more unknown malware is detected, but there are also likely to be false positives.

## 11.1.2 Report

The System Scanner has a comprehensive reporting function. You thus obtain precise information on the results of an on-demand scan. The report file contains all entries of the system as well as alerts and messages of the on-demand scan.

### Note

To be able to establish what actions the System Scanner has performed, when viruses or unwanted programs have been detected, you should activate the report file in the configuration.

## Reporting

### Off

If this option is enabled, the System Scanner does not report the actions and results of the on-demand scan.

### Default

When this option is activated, the System Scanner logs the path and names of the concerning files. In addition, the configuration for the current scan, version information and information on the licensee is written in the report file.

### Extended

When this option is activated, the System Scanner logs alerts and tips in addition to the default information. The report also contains a '(cloud)' suffix to identify the detections from Protection Cloud.

## Complete

When this option is activated, the System Scanner also logs all scanned files. In addition, all files involved as well as alerts and tips are included in the report file.

### Note

If you have to send us a report file at any time (for troubleshooting), please create this report file in this mode.

## 11.2 Real-Time Protection

The **Real-Time Protection** section of the configuration is responsible for the configuration of the on-access scan.

### 11.2.1 Scan

You will normally want to monitor your system constantly. To this end, use the Real-Time Protection (= on-access System Scanner). You can thus scan all files that are copied or opened on the computer "on the fly", for viruses and unwanted programs.

#### *Files*

The Real-Time Protection can use a filter to scan only those files with a certain extension (type).

#### **All files**

If this option is enabled, all files are scanned for viruses or unwanted programs, irrespective of their content and their file extension.

### Note

If **All files** is enabled, the **File extensions** button cannot be selected.

#### **Use smart extensions**

If this option is enabled, the selection of the files scanned for viruses or unwanted programs is automatically chosen by the program. This means that the program decides whether the files are scanned or not based on their content. This procedure is somewhat slower than **Use file extension list**, but more secure, since not only on the basis of the file extension is scanned.

### Note

If **Use smart extensions** is enabled, the **File extensions** button cannot be selected.

## Use file extension list

If this option is enabled, only files with a specified extension are scanned. All file types that may contain viruses and unwanted programs are preset. The list can be edited manually via the "**File extensions**" button. This option is enabled as the default setting and is recommended.

### Note

If this option is enabled and you have deleted all entries from the list with file extensions, this is indicated with the text "No file extensions" under the **File extensions** button.

## File extensions

With the aid of this button, a dialog box is opened in which all file extensions are displayed that are scanned in "**Use file extension list**" mode. Default entries are set for the extensions, but entries can be added or deleted.

### Note

Please note that the file extension list may vary from version to version.

## Scan mode

Here the time for scanning of a file is defined.

## Scan when reading

If this option is enabled, the Real-Time Protection scans the files before they are read or executed by the application or the operating system.

## Scan when writing

If this option is enabled, the Real-Time Protection scans a file when writing. You can only access the file again after this process has been completed.

## Scan when reading and writing

If this option is enabled, the Real-Time Protection scans files before opening, reading and executing and after writing. This option is enabled as the default setting and is recommended.

## Drives

## Monitor network drives

If this option is enabled, files on network drives (mapped drives) such as server volumes, peer drives etc., are scanned.



**Note**

In order not to reduce the performance of your computer too much, the option **Monitor network drives** should only be enabled in exceptional cases.

**Warning**

If this option is disabled, the network drives are **not** monitored. They are no longer protected against viruses or unwanted programs!

**Note**

When files are executed on network drives, they are scanned by the Real-Time Protection irrespective of the setting for the **Monitor network drives** option. In some cases files on network drives are scanned while being opened, even though the **Monitor network drives** option is disabled. Reason: These files are accessed with 'Execute File' rights. If you want to exclude these files or even executed files on network drives from scanning by the Real-Time Protection, enter the files in the list of file objects to be excluded (see: [Real-Time Protection > Scan > Exceptions](#)).

**Enable caching**

If this option is enabled, monitored files on network drives will be made available in the Real-Time Protection's cache. Monitoring of network drives without the caching function is more secure, but does not perform as well as the monitoring of network drives with caching.

*Archives***Scan archives**

If this option is enabled, then archives will be scanned. Compressed files are scanned, then decompressed and scanned again. This option is deactivated by default. The archive scan is restricted by the recursion depth, the number of files to be scanned and the archive size. You can set the maximum recursion depth, the number of files to be scanned and the maximum archive size.

**Note**

This option is deactivated by default, since the process puts heavy demands on the computer's performance. It is generally recommended that archives be checked using an on-demand scan.

**Max. recursion depth**

When scanning archives, the Real-Time Protection uses a recursive scan: Archives in archives are also unpacked and scanned for viruses and unwanted programs. You can

define the recursion depth. The default value for the recursion depth is 1 and is recommended: all files that are directly located in the main archive are scanned.

### **Max. number of files**

When scanning archives, you can restrict the scan to a maximum number of files in the archive. The default value for the maximum number of files to be scanned is 10 and is recommended.

### **Max. size (KB)**

When scanning archives, you can restrict the scan to a maximum archive size to be unpacked. The standard value of 1000 KB is recommended.

## **Action on detection**

You can define the actions to be performed by Real-Time Protection when a virus or unwanted program is detected.

### **Interactive**

If this option is enabled, a desktop notification appears when Real-Time Protection detects a virus or unwanted program. You have the option of removing the detected malware or accessing other possible virus treatment actions via the "**Details**" button. The actions are displayed in a dialog box. This option is enabled as the default setting.

#### *Permitted actions*

In this display box you can specify the virus management actions that should be available as further actions in the dialog box. You must activate the corresponding options for this.

### **Repair**

Real-Time Protection repairs the infected file if possible.

### **Rename**

Real-Time Protection renames the file. Direct access to these files (e.g. with double-click) is therefore no longer possible. The file can be repaired at a later time and renamed again.

### **Quarantine**

Real-Time Protection moves the file to Quarantine. The file can be recovered from Quarantine manager if it has an informative value or - if necessary - sent to the Avira Malware Research Center. Depending on the file, further options are available in the Quarantine manager.

### **Delete**

The file will be deleted. This process is much faster than **Overwrite and delete** (see below).

### **Ignore**

Access to the file is permitted and the file is ignored.

## Overwrite and delete

Real-Time Protection overwrites the file with a default pattern before deleting it. It cannot be restored.

### Warning

If Real-Time Protection is set to **Scan when writing**, the affected file is not written.

## Default

This button allows you to select an action that is activated in the dialog box by default when a virus is detected. Select the action that should be activated by default and click on the "**Default**" button.

### Note

The action **Repair** cannot be selected as the default action.

[Click here for more information.](#)

## Automatic

If this option is enabled, no dialog box in case of a virus detection appears. Real-Time Protection reacts according to the settings you predefine in this section as primary and secondary action.

### Copy file to quarantine before action

If this option is enabled, the Real-Time Protection creates a backup copy before carrying out the requested primary or secondary action. The backup copy is saved in quarantine. It can be restored via the Quarantine manager if it is of informative value. You can also send the backup copy to the Avira Malware Research Center. Depending on the object, more selection options are available in the Quarantine manager.

#### *Primary action*

Primary action is the action performed when the Real-Time Protection finds a virus or an unwanted program. If the "**Repair**" option is selected but the affected file cannot be repaired, the action selected under "**Secondary action**" is performed.

### Note

The **Secondary action** option can only be selected if the **Repair** setting was selected under **Primary action**.

## Repair

If this option is enabled, the Real-Time Protection repairs affected files automatically. If the Real-Time Protection cannot repair an affected file, it carries out the action selected under **Secondary action**.

**Note**

An automatic repair is recommended, but means that the Real-Time Protection modifies files on the workstation.

**Rename**

If this option is enabled, the Real-Time Protection renames the file. Direct access to these files (e.g. with double-click) is therefore no longer possible. Files can later be repaired and given their original names again.

**Quarantine**

If this option is enabled, the Real-Time Protection moves the file to Quarantine. The files in this directory can later be repaired or - if necessary - sent to the Avira Malware Research Center.

**Delete**

If this option is enabled, the file is deleted. This process is much faster than **Overwrite and delete**.

**Ignore**

If this option is enabled, access to the file is allowed and the file is left as it is.

**Warning**

The affected file remains active on your workstation! It may cause serious damage on your workstation!

**Overwrite and delete**

If this option is enabled, the Real-Time Protection overwrites the file with a default pattern and then deletes it. It cannot be restored.

**Deny access**

If this option is enabled, the Real-Time Protection only enters the detection in the [report file](#) if the report function is enabled. In addition, the Real-Time Protection writes an entry in the [Event log](#), if this option is enabled.

**Warning**

If Real-Time Protection is set to **Scan when writing**, the affected file is not written.

*Secondary action*

The option **Secondary action** can only be selected if the **Repair** option was selected under **Primary action**. With this option it can now be decided what is to be done with the affected file if it cannot be repaired.

### Rename

If this option is enabled, the Real-Time Protection renames the file. Direct access to these files (e.g. with double-click) is therefore no longer possible. Files can later be repaired and given their original names again.

### Quarantine

If this option is enabled, the Real-Time Protection moves the file to Quarantine. The files can later be repaired or - if necessary - sent to the Avira Malware Research Center.

### Delete

If this option is enabled, the file is deleted. This process is much faster than **Overwrite and delete**.

### Ignore

If this option is enabled, access to the file is allowed and the file is left as it is.

#### Warning

The affected file remains active on your workstation! It may cause serious damage on your workstation!

### Overwrite and delete

If this option is enabled, the Real-Time Protection overwrites the file with a default pattern and then deletes it. It cannot be restored.

### Deny access

If this option is enabled, the affected file is not written; the Real-Time Protection only enters the detection in the [report file](#) if the report function is enabled. In addition, the Real-Time Protection writes an entry in the [Event log](#), if this option is enabled.

#### Note

If you have selected **Delete** or **Overwrite and delete** as the primary or secondary action, please note: In the case of heuristic hits, the affected files are not deleted, but are instead moved to quarantine.

## Further actions

### Use event log

If this option is enabled, an entry is added to the Windows event log for every detection. The events can be called up in the Windows event viewer. This option is enabled as the default setting.

## Exceptions

With these options you can configure exception objects for the Real-Time Protection (on-access scan). The relevant objects are then not included in the on-access scan. The Real-Time Protection can ignore file accesses to these objects during the on-access scan via the list of processes to be omitted. This is useful, for example, with databases or backup solutions.

Please note the following when specifying processes and file objects to be omitted: The list is processed from top to bottom. The longer the list is, the more processor time is required for processing the list for each access. Therefore, keep the list as short as possible.

### *Processes to be omitted by the Real-Time Protection*

All file accesses of processes in this list are excluded from monitoring by Real-Time Protection.

## Input box

In this field, enter the name of the process that is to be ignored by the real-time scan. No process is entered as the default setting.

The specified path and file name of the process should contain a maximum of 255 characters. You can enter up to 128 processes. The entries in the list must not result in more than 6000 characters in total.

When entering the process, Unicode symbols are accepted. You can therefore enter process or directory names containing special symbols.

Drive information must be entered as follows: [Drive letter]:\

The colon symbol (:) is only used to specify drives.

When specifying the process, you can use the wildcards \* (any number of characters) and ? (a single character).

```
C:\Program Files\Application\application.exe  
C:\Program Files\Application\applicatio?.exe  
C:\Program Files\Application\applic*.exe  
C:\Program Files\Application\*.exe
```

To avoid the process being excluded globally from monitoring by Real-Time Protection, specifications exclusively comprising the following characters are invalid: \* (asterisk), ? (question mark), / (forward slash), \ (backslash), . (dot), : (colon).

You have the option of excluding processes from monitoring by the Real-Time Protection without full path details. For example: `application.exe`

This however only applies to processes where the executable files are located on hard disk drives.

Full path details are required for processes where the executable files are located on connected drives, e.g. network drives. Please note the general information on the notation of [Exceptions on connected network drives](#).

Do not specify any exceptions for processes where the executable files are located on dynamic drives. Dynamic drives are used for removable disks, such as CDs, DVDs or USB sticks.

**Warning**

Please note that all file accesses done by processes recorded in the list are excluded from the scan for viruses and unwanted programs!



The button opens a window in which you can select an executable file.

**Processes**

The "**Processes**" button opens the "**Process selection**" window in which the running processes are displayed.

**Add**

With this button, you can add the process entered in the input box to the display window.

**Delete**

With this button you can delete a selected process from the display window.

*File objects to be omitted by the Real-Time Protection*

All file accesses to objects in this list are excluded from monitoring by the Real-Time Protection.

**Input box**

In this box you can enter the name of the file object that is not included in the on-access scan. No file object is entered as the default setting.

The entries in the list must have no more than 6000 characters in total.

When specifying file objects to be omitted, you can use the wildcards\* (any number of characters) and ? (a single character): Individual file extensions can also be excluded (including wildcards):

```
C:\Directory\*.mdb  
*.mdb  
*.md?  
*.xls*  
C:\Directory\*.log
```

Directory names must end with a backslash \.

If a directory is excluded, all its sub-directories are automatically also excluded.

For each drive you can specify a maximum of 20 exceptions by entering the complete path (starting with the drive letter). For example:

```
C:\Program Files\Application\Name.log
```

The maximum number of exceptions without a complete path is 64. For example:

```
*.log  
\computer1\C\directory1
```

In case of dynamic drives that are mounted as a directory on another drive, the alias of the operating system for the integrated drive in the list of the exceptions has to be used, e.g.:

```
\Device\HarddiskDmVolumes\PhysicalDmVolumes\BlockVolume1\
```

If you use the mount point itself, for example, `C:\DynDrive`, the dynamic drive will be scanned nonetheless. You can determine the alias of the operating system to be used from the Real-Time Protection report file.



The button opens a window in which you can select the file object to be excluded.

## Add

With this button, you can add the file object entered in the input box to the display window.

## Delete

With this button you can delete a selected file object from the display window.

## Please note the further information when specifying exceptions:

In order to also exclude objects when they are accessed with short DOS file names (DOS name convention 8.3), the relevant short file name must also be entered in the list.

A file name that contains wildcards may not be terminated with a backslash. For example:

```
C:\Program Files\Application\applic*.exe\
```

This entry is not valid and not treated as an exception!

Please note the following with regard to **exceptions on connected network drives**: If you use the drive letter of the connected network drive, the files and folders specified are NOT excluded from the Real-Time Protection scan. If the UNC path in the list of exceptions differs from the UNC path used to connect to the network drive (IP address specification in the list of exceptions – specification of computer name for connection to network drive), the specified folders and files are NOT excluded by the Real-Time Protection scan. Locate the relevant UNC path in the Real-Time Protection report file:

```
\\<Computer name>\<Enable>\ - OR - \\<IP address>\<Enable>\
```

You can locate the path Real-Time Protection uses to scan for infected files in the Real-Time Protection report file. Indicate exactly the same path in the list of exceptions.



Proceed as follows: Set the protocol function of the Real-Time Protection to **Complete** in the configuration under [Real-Time Protection > Report](#). Now access the files, folders, mounted drives or connected network drives with the activated Real-Time Protection. You can now read the path to be used from the Real-Time Protection report file. The report file can be accessed in the Control Center under Local protection > Real-Time Protection.

## Heuristic

This configuration section contains the settings for the heuristic of the scan engine.

Avira products contain very powerful heuristics that can proactively uncover unknown malware, i.e. before a special virus signature to combat the damaging element has been created and before a virus guard update has been sent. Virus detection involves an extensive analysis and investigation of the affected codes for functions typical of malware. If the code being scanned exhibits these characteristic features, it is reported as being suspicious. This does not necessarily mean that the code is in fact malware. False positives do sometimes occur. The decision on how to handle affected code is to be made by the user, e.g. based on his or her knowledge of whether the source of the code is trustworthy or not.

### *Macrovirus heuristics*

#### Macrovirus heuristics

Your Avira product contains a highly powerful macrovirus heuristic. If this option is enabled, all macros in the relevant document are deleted in the event of a repair, alternatively suspect documents are only reported, i.e. you receive an alert. This option is enabled as the default setting and is recommended.

### *Advanced Heuristic Analysis and Detection (AHeAD)*

#### Enable AHeAD

Your Avira program contains a very powerful heuristic in the form of Avira AHeAD technology, which can also detect unknown (new) malware. If this option is enabled, you can define how "aggressive" this heuristic should be. This option is enabled as the default setting.

##### Low detection level

If this option is enabled, slightly less unknown malware is detected, the risk of false alerts is low in this case.

##### Medium detection level

This option combines a strong detection level with a low risk of false alerts. Medium is the default setting if you have selected the use of this heuristic.

##### High detection level

If this option is enabled, significantly more unknown malware is detected, but there are also likely to be false positives.

## 11.2.2 Report

Real-Time Protection includes an extensive logging function to provide the user or administrator with exact notes about the type and manner of a detection.

### *Reporting*

This group allows for the content of the report file to be determined.

#### **Off**

If this option is enabled, then Real-Time Protection does not create a log. It is recommended that you should turn off the logging function only in exceptional cases, such as if you are executing trials with multiple viruses or unwanted programs.

#### **Default**

If this option is enabled, Real-Time Protection records important information (concerning detections, alerts and errors) in the report file, with less important information ignored for improved clarity. This option is enabled as the default setting.

#### **Extended**

If this option is enabled, Real-Time Protection logs less important information to the report file as well.

#### **Complete**

If this option is enabled, Real-Time Protection logs all available information in the report file, including file size, file type, date, etc.

### *Limit report file*

#### **Limit size to n MB**

If this option is enabled, the report file can be limited to a certain size. Permitted values are between 1 and 100 MB. Around 50 kilobytes of extra space are allowed when limiting the size of the report file to minimize the use of system resources. If the size of the log file exceeds the indicated size by more than 50 kilobytes, then old entries are deleted until the indicated size minus 50 kilobytes is reached.

#### **Backup report file before shortening**

If this option is enabled, the report file is backed up before shortening.

#### **Write configuration in report file**

If this option is enabled, the configuration of the on-access scan is recorded in the report file.

**Note**

If you have not specified any report file restriction, a new report file is automatically created when the report file reaches 100 MB. A backup of the old report file is created. Up to three backups of old report files are saved. The oldest backups are deleted first.

## 11.3 Update

In the **Update** section you can configure the automatic receiving of updates. You can specify various update intervals.

### *Automatic update*

**All n Day(s) / Hour(s) / Minute(s)**

In this box you can specify the interval at which the automatic update is performed. To change the update interval, highlight one of the time options in the box and change it using the arrow keys to the right of the input box.

**Also start job when Internet connection is established**

If this option is enabled, in addition to the specified update interval, the update job is performed every time an Internet connection is established.

**Repeat job if the time has already expired**

If this option is enabled, past update jobs are performed that could not be performed at the time specified, for example because the computer was switched off.

### 11.3.1 Web server

**Web server**

The update can be performed directly via a web server on the Internet.

#### *Web server connection*

**Use existing connection (network)**

This setting is displayed if your connection is used via a network.

**Use the following connection**

This setting is displayed if you define your connection individually.

The Updater automatically detects which connection options are available. Connection options that are not available are grayed out and cannot be activated. A dial-up connection can be established manually via a phone book entry in Windows, for example.

**User**

Enter the user name of the selected account.

**Password**

Enter the password for this account. For security reasons, the actual characters you type in this space are replaced by asterisks (\*).

**Note**

If you have forgotten an existing Internet account name or password, contact your Internet Service Provider.

**Note**

The automatic dial-up of the updater through so-called dial-up tools (e.g. SmartSurfer, Oleco, etc.) is currently not yet available.

**Terminate a dial-up connection that was set up for the update**

If this option is enabled, the dial-up connection made for the update is automatically interrupted again as soon as the download has been successfully performed.

**Note**

This option is only available under Windows XP. Under newer operating systems the dial-up connection opened for the update is always terminated as soon as the download has been performed.

**Proxy settings**

*Proxy server*

**Do not use a proxy server**

If this option is enabled, your connection to the web server is not established via a proxy server.

**Use proxy system settings**

When the option is enabled, the current Windows system settings are used for the connection to the web server via a proxy server. Configure the Windows system settings to use a proxy server under **Control panel > Internet options > Connections > LAN settings**. You can also access the Internet options in the **Extras** menu in Internet Explorer.

**Warning**

If you are using a proxy server which requires authentication, enter all the

required data under the option **Use this proxy server**. The **Use proxy system settings** option can only be used for proxy servers without authentication.

### Use this proxy server

If your web server connection is set up via a proxy server, you can enter the relevant information here.

#### Address

Enter the computer name or IP address of the proxy server you want to use to connect to the web server.

#### Port

Please enter the port number of the proxy server you want to use to connect to the web server.

#### Login name

Enter a user name to log in on the proxy server.

#### Login password

Enter the relevant password for logging in on the proxy server here. For security reasons, the actual characters you type in this space are replaced by asterisks (\*).

Examples:

Address: `proxy.domain.com` Port: 8080

Address: `192.168.1.100` Port: 3128

## 11.4 FireWall

Avira Antivirus Suite allows you to configure to manage the Windows Firewall (starting from Windows 7):

- Avira FireWall
- [Windows Firewall](#)

### 11.4.1 Windows Firewall

The **FireWall** section under **Configuration > Internet Protection** is responsible for configuration of the Windows Firewall, starting from Windows 7.

#### Network profiles

#### Network profiles

Windows Firewall blocks the unauthorized access of programs and apps to your computer based on three network location profiles:

- **Private network**: for home or office networks
- **Public network**: for public places' networks
- **Domain network**: for networks with a domain controller

You can manage these profiles from the configuration of your Avira product under **Internet protection > Windows Firewall > Network profiles**.

For further information about these network profiles, please visit the official Microsoft website.

### **Warning**

Windows Firewall applies the same rules for all networks that belong to the same network location, this means that, if you allow to run a program or application, this program or application will also be granted access in all the networks that have the same profile.

## **Private network**

### *Private network settings*

The private network settings manage the access other computers or devices in your home or office network have to your computer. These settings allow by default the users of the private network to see and access your computer.

### **Enable**

If this option is enabled, Windows Firewall is activated and working through the Avira product.

### **Block all incoming connections**

If this option is enabled, Windows Firewall will reject all unsolicited attempts to connect to your computer, including incoming connections from allowed applications.

### **Notify me when a new app is blocked**

If this option is enabled, you will receive a notification every time that Windows Firewall blocks a new program or app.

### **Disable (not recommended)**

If this option is enabled, Windows Firewall is deactivated. This option is not recommended, it puts your computer at risk.

## **Public network**

### *Public network settings*

The public network settings manage the access other computers or devices in public places' networks have to your computer. These settings do not allow, by default, the users of the public network to see and access your computer.

**Enable**

If this option is enabled, Windows Firewall is activated and working through the Avira product.

**Block all incoming connections**

If this option is enabled, Windows Firewall will reject all unsolicited attempts to connect to your computer, including incoming connections from allowed applications.

**Notify me when a new app is blocked**

If this option is enabled, you will receive a notification every time that Windows Firewall blocks a new program or app.

**Disable (not recommended)**

If this option is enabled, Windows Firewall is deactivated. This option is not recommended, it puts your computer at risk.

**Domain network***Domain network settings*

The domain network settings manage the access other computers or devices have to your computer in a network that authenticates through a domain controller. These settings allow, by default, authenticated users of the domain to see and access your computer.

**Enable**

If this option is enabled, Windows Firewall is activated and working through the Avira product.

**Block all incoming connections**

If this option is enabled, Windows Firewall will reject all unsolicited attempts to connect to your computer, including incoming connections from allowed applications.

**Notify me when a new app is blocked**

If this option is enabled, you will receive a notification every time that Windows Firewall blocks a new program or app.

**Disable (not recommended)**

If this option is enabled, Windows Firewall is deactivated. This option is not recommended, it puts your computer at risk.

**Note**

This option is only available if your computer is connected to a network with a domain controller.

**Application rules**

If you click the link under **Windows Firewall > Application rules**, you will be redirected to the menu **Allowed apps and features** of the Windows Firewall configuration.

**Advanced settings**

If you click the link under **Windows Firewall > Advanced settings**, you will be redirected to the menu **Windows Firewall with Advanced Security** of the Windows Firewall configuration.

## 11.5 Web Protection

The **Web Protection** section under **Configuration > Internet Protection** is responsible for the configuration of the Web Protection.

### 11.5.1 Scan

Web Protection protects you against viruses or malware that reach your computer from web pages that you load on your web browser from the Internet. The **Scan** options can be used to set the behavior of the Web Protection component.

#### *Scan*

**Enable IPv6 support**

If this option is enabled, Internet Protocol version 6 is supported by the Web Protection. This option is not available for new or changed installations under Windows 8.

#### *Drive-by protection*

Drive-by protection allows you to make settings to block I-Frames, also known as inline frames. I-Frames are HTML elements, i.e. elements of Internet pages that delimit an area of a web page. I-Frames can be used to load and display different web content - usually other URLs - as independent documents in a sub-window of the browser. I-Frames are mostly used for banner advertising. In some cases, I-Frames are used to conceal malware. In these cases the area of the I-Frame is mostly invisible or almost invisible in the browser. The **Block suspicious I-frames** option allows you to check and block the loading of I-Frames.



## Block suspicious I-frames

If this option is enabled, I-Frames on the web pages you request are scanned according to certain criteria. If there are suspect I-Frames on a requested web page, the I-Frame is blocked. An error message is displayed in the I-Frame window.

## Action on detection

You can define the actions to be performed by Web Protection when a virus or unwanted program is detected.

### Interactive

If this option is enabled, a dialog box appears when a virus or unwanted program is detected during an on-demand scan, in which you can choose what is to be done with the affected file. This option is enabled as the default setting.

### Show progress bar

If this option is enabled, a desktop notification appears with a download progress bar if a download of website content exceeds a 20 second timeout. This desktop notification is designed in particular for downloading websites with larger data volumes: If you are surfing with Web Protection, website contents are not downloaded incrementally in the Internet browser, as they are scanned for viruses and malware before being displayed in the Internet browser. This option is disabled as the default setting.

[Click here for more information.](#)

### Automatic

If this option is enabled, no dialog box in case of a virus detection appears. Web Protection reacts according to the settings you predefine in this section as primary and secondary action.

#### *Primary action*

The primary action is the action performed when Web Protection finds a virus or an unwanted program.

### Deny access

The website requested from the web server and/ or any data or files transferred are not sent to your web browser. An error message to notify you that access has been denied is displayed in the web browser. Web Protection logs the detection to the report file if the [report function](#) is activated.

### Move to quarantine

In the event of a virus or malware being detected, the website requested from the web server and/ or the transferred data and files are moved into quarantine. The affected file can be recovered from the quarantine manager if it has any informative value or - if necessary - sent to the Avira Malware Research Center.

## Ignore

The website requested from the web server and/ or the data and files that were transferred are forwarded on by Web Protection to your web browser. Access to the file is permitted and the file is ignored.

### Warning

The affected file remains active on your workstation! It may cause serious damage on your workstation!

## Blocked requests

In **Blocked requests** you can specify the file types and MIME types (content types for the transferred data) to be blocked by Web Protection. The Web filter lets you block known phishing and malware URLs. Web Protection prevents the transfer of data from the Internet to your computer system.

*Web Protection blocks the following file types / MIME-Types*

All file types and MIME types (content types for the transferred data) in the list are blocked by Web Protection.

## Input box

In this box, enter the names of the MIME types and file types you want Web Protection to block. For file types, enter the file extension, e.g. **.htm**. For MIME types, indicate the media type and, where applicable, sub-type. The two statements are separated from one another by a single slash, e.g. **video/mpeg** or **audio/x-wav**.

### Note

Files which are already stored on your system as temporary Internet files and blocked by Web Protection can, however, be downloaded locally from the Internet by your computer's Internet browser. Temporary Internet files are files saved on your computer by the Internet browser so that websites can be accessed more quickly.

### Note

The list of blocked file and MIME types is ignored if they are entered in the list of excluded file and MIME types under [Web Protection > Scan > Exceptions](#).

**Note**

No wildcards (\* for any number of characters or ? for a single character) can be used when entering file types and MIME types.

MIME types: Examples for media types:

- `text` = for text files
- `image` = for graphics files
- `video` = for video files
- `audio` = for sound files
- `application` = for files linked to a particular program

Examples of excluded file and MIME types

- `application/octet-stream` = `application/octet-stream` MIME type files (executable files `*.bin`, `*.exe`, `*.com`, `*.dll`, `*.class`) are blocked by Web Protection.
- `application/olescript` = `application/olescript` MIME type files (ActiveX script-files `*.axs`) are blocked by Web Protection.
- `.exe` = All files with the extension `.exe` (executable files) are blocked by Web Protection.
- `.msi` = All files with the extension `.msi` (Windows Installer files) are blocked by Web Protection.

**Add**

The button allows you to copy MIME and file types from the input field into the display window.

**Delete**

The button deletes a selected entry from the list. This button is inactive if no entry is selected.

*Web filter*

The web filter is based on an internal database, updated daily, that classifies URLs according to content.

**Activate web filter**

When the option is enabled, all URLs matching the selected categories in the web filter list are blocked.

**Web filter list**

In the web filter list you can select the content categories whose URLs are to be blocked by Web Protection.

**Note**

The web filter is ignored for entries in the list of excluded URLs under [Web Protection > Scan > Exceptions](#).

**Note**

**Spam URLs** are URLs sent with spam emails. The **Fraud / Deception** category covers web pages with “Subscription Expires” and other offers of services whose costs are hidden by the provider.

## Exceptions

These options allow you to set exceptions based on MIME types (content types for the transferred data) and file types for URLs (Internet addresses) for scanning by Web Protection. The MIME types and URLs specified are ignored by Web Protection, i.e. that data is not scanned for viruses and malware when it is transferred to your computer system.

### *MIME types skipped by Web Protection*

In this field you can select the MIME types (content types for the transferred data) to be ignored by Web Protection during scanning.

### *File types/MIME types skipped by Web Protection (user-defined)*

All MIME types (content types for the transferred data) in the list are ignored by Web Protection during scanning.

## Input box

In this box you can input the name of the MIME types and file types to be ignored by Web Protection during scanning. For file types, enter the file extension, e.g. **.htm**. For MIME types, indicate the media type and, where applicable, sub-type. The two statements are separated from one another by a single slash, e.g. **video/mpeg** or **audio/x-wav**.

**Note**

No wildcards (\* for any number of characters or ? for a single character) can be used when entering file types and MIME types.

**Warning**

All file types and content types on the exclusion list are downloaded into the Internet browser without further scanning of the blocked requests (list of file and MIME types to be blocked in [Web Protection > Scan > Blocked requests](#)) or by

Web Protection: For all entries on the exclusion list, the entries on the list of file and MIME types to be blocked are ignored. No scan for viruses and malware is performed.

MIME types: Examples for media types:

- `text` = for text files
- `image` = for graphics files
- `video` = for video files
- `audio` = for sound files
- `application` = for files linked to a particular program

Examples of excluded file and MIME types:

- `audio/` = All audio media type files are excluded from Web Protection scans
- `video/quicktime` = All Quicktime sub-type video files (\*.qt, \*.mov) are excluded from Web Protection scans
- `.pdf` = All Adobe PDF files are excluded from Web Protection scans.

### Add

The button allows you to copy MIME and file types from the input field into the display window.

### Delete

The button deletes a selected entry from the list. This button is inactive if no entry is selected.

### *URLs skipped by Web Protection*

All URLs in this list are excluded from Web Protection scans.

### Input box

In this box you can input URLs (Internet addresses) to be excluded from Web Protection scans, e.g. `www.domainname.com`. You can specify parts of the URL, using leading or following dots to indicate the domain level: `.domainname.com` for all pages and all subdomains of the domain. Indicate websites with any top-level domain (`.com` or `.net`) with a following dot: `domainname.`. If you indicate a string without a leading or concluding dot, the string is interpreted as a top-level domain, e.g. `net` for all NET domains (`www.domain.net`).

#### Note

You can also use the wildcard `*` for any number of characters when specifying URLs. You can also use leading or following dots in combination with wildcards to indicate the domain level:

```
.domainname.*  
*.domainname.com  
.*name*.com (valid but not recommended)
```

Specifications without dots, like `*name*`, are interpreted as part of a top-level domain and are not advisable.

### Warning

All websites on the list of excluded URLs are downloaded into the Internet browser without further scanning by the web filter or by Web Protection: For all entries in the list of excluded URLs, the entries in the web filter (see [Web Protection > Scan > Blocked requests](#)) are ignored. No scan for viruses and malware is performed. Only trusted URLs should therefore be excluded from Web Protection scans.

## Add

The button allows you to copy the URL entered in the input field (Internet address) to the viewer window.

## Delete

The button deletes a selected entry from the list. This button is inactive if no entry is selected.

## Examples: Skipped URLs

- `www.avira.com -OR- www.avira.com/*`  
= All URLs with the domain `www.avira.com` are excluded from Web Protection scans: `www.avira.com/en/pages/index.php`, `www.avira.com/en/support/index.html`, `www.avira.com/en/download/index.html`, etc.  
URLs with the domain `www.avira.de` are not excluded from Web Protection scans.
- `avira.com -OR- *.avira.com`  
= All URLs with the second and top-level domain `avira.com` are excluded from Web Protection scans: The specification implies all existing subdomains for `.avira.com`: `www.avira.com`, `forum.avira.com`, etc.
- `avira. -OR- *.avira.*`  
= All URLs with the second-level domain `avira` are excluded from Web Protection scans: The specification implies all existing top-level domains or subdomains for `.avira`: `www.avira.com`, `www.avira.de`, `forum.avira.com`, etc.
- `.*domain*.*`  
All URLs containing a second-level domain with the string `domain` are excluded from Web Protection scans: `www.domain.com`, `www.new-domain.de`, `www.sample-domain1.de`, ...
- `net -OR- *.net`  
= All URLs with the top-level domain `net` are excluded from Web Protection scans: `www.name1.net`, `www.name2.net`, etc.

**Warning**

Enter the URLs you want to exclude from the Web Protection scan as precisely as possible. Avoid specifying an entire top-level domain or parts of a second-level domain because there is a risk that Internet pages that distribute malware and undesirable programs will be excluded from the Web Protection scan through global specifications under exclusions. You are recommended to specify at least the complete second-level domain and the top-level domain:  
`domainname.com`

**Heuristic**

This configuration section contains the settings for the heuristic of the scan engine.

Avira products contain very powerful heuristics that can proactively uncover unknown malware, i.e. before a special virus signature to combat the damaging element has been created and before a virus guard update has been sent. Virus detection involves an extensive analysis and investigation of the affected codes for functions typical of malware. If the code being scanned exhibits these characteristic features, it is reported as being suspicious. This does not necessarily mean that the code is in fact malware. False positives do sometimes occur. The decision on how to handle affected code is to be made by the user, e.g. based on his or her knowledge of whether the source of the code is trustworthy or not.

**Macrovirus heuristic**

Your Avira product contains a highly powerful macrovirus heuristic. If this option is enabled, all macros in the relevant document are deleted in the event of a repair, alternatively suspect documents are only reported, i.e. you receive an alert. This option is enabled as the default setting and is recommended.

*Advanced Heuristic Analysis and Detection (AHeAD)***Enable AHeAD**

Your Avira program contains a very powerful heuristic in the form of Avira AHeAD technology, which can also detect unknown (new) malware. If this option is enabled, you can define how "aggressive" this heuristic should be. This option is enabled as the default setting.

**Low detection level**

If this option is enabled, slightly less unknown malware is detected, the risk of false alerts is low in this case.

**Medium detection level**

This option combines a strong detection level with a low risk of false alerts. Medium is the default setting if you have selected the use of this heuristic.

**High detection level**

If this option is enabled, significantly more unknown malware is detected, but there are also likely to be false positives.

**11.5.2 Report**

The Web Protection includes an extensive logging function to provide the user or administrator with exact notes about the type and manner of a detection.

*Reporting*

This group allows for the content of the report file to be determined.

**Off**

If this option is enabled, then Web Protection does not create a log. It is recommended that you should turn off the logging function only in exceptional cases, such as if you are executing trials with multiple viruses or unwanted programs.

**Default**

If this option is enabled, Web Protection records important information (concerning detections, alerts and errors) in the report file, with less important information ignored for improved clarity. This option is enabled as the default setting.

**Extended**

If this option is enabled, Web Protection logs less important information to the report file as well.

**Complete**

If this option is enabled, Web Protection logs all available information in the report file, including file size, file type, date, etc.

*Limit report file***Limit size to n MB**

If this option is enabled, the report file can be limited to a certain size; possible values: Permitted values are between 1 and 100 MB. Around 50 kilobytes of extra space are allowed when limiting the size of the report file to minimize the use of system resources. If the size of the log file exceeds the indicated size by more than 50 kilobytes, old entries are then deleted until the indicated size has been reduced by 20%.

**Write configuration in report file**

If this option is enabled, the configuration of the on-access scan is recorded in the report file.



**Note**

If you have not specified any report file restriction, older entries are automatically deleted when the report file reaches 100 MB. Entries are deleted until the size of the report file reaches 80 MB.

## 11.6 Mail Protection

The **Mail Protection** section of the Configuration is responsible for the configuration of the Mail Protection.

### 11.6.1 Scan

Use Mail Protection to scan incoming emails for viruses and malware. Outgoing emails can be scanned for viruses and malware by Mail Protection.

#### Scan incoming emails

If this option is enabled, incoming emails are scanned for viruses and malware. Mail Protection supports POP3 and IMAP protocols. Enable the inbox account used by your email client to receive emails for monitoring by Mail Protection.

##### Monitor POP3 accounts

If this option is enabled, the POP3 accounts are monitored on the specified ports.

##### Monitored ports

In this field you should enter the port to be used as the inbox by the POP3 protocol. Multiple ports are separated by commas.

##### Default

This button resets the specified port to the default POP3 port.

##### Monitor IMAP accounts

If this option is enabled, the IMAP accounts are monitored on the specified ports.

##### Monitored ports

In this field you should enter the port to be used as the inbox by the IMAP protocol. Multiple ports are separated by commas.

##### Default

This button resets the specified port to the default IMAP port.

#### Scan outgoing emails (SMTP)

If this option is enabled, outgoing emails are scanned for viruses and malware.

### Monitored ports

In this field you should enter the port to be used as the outbox by the SMTP protocol. Multiple ports are separated by commas.

### Default

This button resets the specified port to the default SMTP port.

#### Note

To verify the protocols and ports used, call up the properties of your email accounts in your email client program. Default ports are mostly used.

### Enable IPv6 support

If this option is enabled, Internet Protocol version 6 is supported by the Mail Protection. (Option not available for new or changed installations under Windows 8.)

### Action on detection

This configuration section contains settings for actions performed when Mail Protection finds a virus or unwanted program in an email or in an attachment.

#### Note

These actions are performed both when a virus is detected in incoming emails and when a virus is detected in outgoing emails.

### Interactive

If this option is enabled, a dialog box appears when a virus or unwanted program is detected in an email or attachment in which you can choose what is to be done with the email or attachment concerned. This option is enabled as the default setting.

### Show progress bar

If this option is enabled, the Mail Protection shows a progress bar during downloading of emails. This option can only be enabled if the option "**Interactive**" has been selected.

### Automatic

If this option is enabled, you are no longer notified when a virus or unwanted program is found. Mail Protection reacts according to the settings you define in this section.

#### *Affected emails*

The action chosen for "*Affected emails*" is performed when the Mail Protection finds a virus or an unwanted program in an email. If the option "**Ignore**" is selected, it is also possible, under "*Affected attachments*", to select the process for dealing with a virus or unwanted program detected in an attachment.

**Delete**

If this option is enabled, the affected email is automatically deleted if a virus or unwanted program is found. The body of the email is replaced by the [default text](#) given below. The same applies to all attachments included; these are also replaced by a [default text](#).

**Ignore**

If this option is enabled, the affected email is ignored despite detection of a virus or unwanted program. However, you can decide what is to be done with the affected attachment.

**Move to quarantine**

If this option is enabled, the complete email including all attachments is placed in Quarantine if a virus or unwanted program is found. If required, it can later be restored. The affected email itself is deleted. The body of the email is replaced by the [default text](#) given below. The same applies to all attachments included; these are also replaced by a [default text](#).

*Affected attachments*

The option "*Affected attachments*" can only be selected if the setting "**Ignore**" has been selected under "*Affected emails*". With this option it is now possible to decide what is to be done if a virus or unwanted program is found in an attachment.

**Delete**

If this option is enabled, the affected attachment is deleted if a virus or unwanted program is found and replaced by a [default text](#).

**Ignore**

If this option is enabled, the attachment is ignored despite detection of a virus or unwanted program and delivered.

**Warning**

If you select this option, you have no protection against viruses and unwanted programs by the Mail Protection. Only select this item if you are certain you know what you are doing. Disable the preview in your email program, never open attachments by double-clicking!

**Move to quarantine**

If this option is enabled, the affected attachment is placed in Quarantine and then deleted (replaced by a [default text](#)). If required, the affected attachment(s) can later be restored.

**Further actions**

This configuration section contains further settings for actions performed when Mail Protection finds a virus or unwanted program in an email or in an attachment.

**Note**

These actions are performed exclusively when a virus is detected in incoming emails.

**Default text for deleted and moved emails**

The text in this box is inserted in the email as a message instead of the affected email. You can edit this message. A text may contain a maximum of 500 characters.

You can use the following key combination for formatting:

**Ctrl + Enter** = inserts a line break.

**Default**

The button inserts a pre-defined default text in the edit box.

**Default text for deleted and moved attachments**

The text in this box is inserted in the email as a message instead of the affected attachment. You can edit this message. A text may contain a maximum of 500 characters.

You can use the following key combination for formatting:

**Ctrl + Enter** = inserts a line break.

**Default**

The button inserts a pre-defined default text in the edit box.

**Heuristic**

This configuration section contains the settings for the heuristic of the scan engine.

Avira products contain very powerful heuristics that can proactively uncover unknown malware, i.e. before a special virus signature to combat the damaging element has been created and before a virus guard update has been sent. Virus detection involves an extensive analysis and investigation of the affected codes for functions typical of malware. If the code being scanned exhibits these characteristic features, it is reported as being suspicious. This does not necessarily mean that the code is in fact malware. False positives do sometimes occur. The decision on how to handle affected code is to be made by the user, e.g. based on his or her knowledge of whether the source of the code is trustworthy or not.

**Macrovirus heuristic**

Your Avira product contains a highly powerful macrovirus heuristic. If this option is enabled, all macros in the relevant document are deleted in the event of a repair, alternatively suspect documents are only reported, i.e. you receive an alert. This option is enabled as the default setting and is recommended.

*Advanced Heuristic Analysis and Detection (AHeAD)*

## Enable AHeAD

Your Avira program contains a very powerful heuristic in the form of Avira AHeAD technology, which can also detect unknown (new) malware. If this option is enabled, you can define how "aggressive" this heuristic should be. This option is enabled as the default setting.

### Low detection level

If this option is enabled, slightly less unknown malware is detected, the risk of false alerts is low in this case.

### Medium detection level

This option combines a strong detection level with a low risk of false alerts. Medium is the default setting if you have selected the use of this heuristic.

### High detection level

If this option is enabled, significantly more unknown malware is detected, but there are also likely to be false positives.

## 11.6.2 General

### Exceptions

#### Scanning exceptions

This table shows you the list of email addresses excluded from scanning by Mail Protection (white list).

#### Note

The list of exceptions is used exclusively by Mail Protection with regard to incoming emails.

#### *Scanning exceptions*

#### Input box

In this box you enter the email address that you want to add to the list of email addresses not to be scanned. Depending on your settings, the email address will no longer be scanned in future by the Mail Protection.

#### Add

With this button you can add the email address entered in the input box to the list of email addresses not to be scanned.

#### Delete

This button deletes a highlighted email address from the list.

**Email address**

Email that is no longer to be scanned.

**Malware**

When this option is enabled, the email address is no longer scanned for malware.

**Up**

You can use this button to move a highlighted email address to a higher position. If no entry is highlighted or the highlighted address is at the first position in the list, this button is not enabled.

**Down**

You can use this button to move a highlighted email address to a lower position. If no entry is highlighted or the highlighted address is at the last position in the list, this button is not enabled.

**Cache**

The Mail Protection cache contains data regarding the scanned emails that is displayed as statistical data in the Control Center under **Mail Protection**.

**Maximum number of emails in the cache**

This field is used to set the maximum number of emails that are stored by Mail Protection in the cache. Emails are deleted oldest first.

**Maximum days for an email to be stored**

The maximum storage period of an email in days is entered in this box. After this time, the email is removed from the cache.

**Empty Cache**

Click on this button to delete the emails stored in the cache.

### 11.6.3 Report

Mail Protection includes an extensive logging function to provide the user or administrator with exact notes about the type and manner of a detection.

*Reporting*

This group allows for the content of the report file to be determined.

**Off**

If this option is enabled, then Mail Protection does not create a log. It is recommended that you should turn off the logging function only in exceptional cases, such as if you are executing trials with multiple viruses or unwanted programs.

**Default**

If this option is enabled, Mail Protection records important information (concerning detections, alerts and errors) in the report file, with less important information ignored for improved clarity. This option is enabled as the default setting.

**Extended**

If this option is enabled, Mail Protection logs less important information to the report file as well.

**Complete**

If this option is enabled, Mail Protection logs all information to the report file.

*Limit report file***Limit size to n MB**

If this option is enabled, the report file can be limited to a certain size; possible values: Permitted values are between 1 and 100 MB. Around 50 kilobytes of extra space are allowed when limiting the size of the report file to minimize the use of system resources. If the size of the log file exceeds the indicated size by more than 50 kilobytes, then old entries are deleted until the indicated size minus 50 kilobytes is reached.

**Backup report file before shortening**

If this option is enabled, the report file is backed up before shortening.

**Write configuration in report file**

If this option is enabled, the Mail Protection configuration is recorded in the report file.

**Note**

If you have not specified any report file restriction, a new report file is automatically created when the report file reaches 100 MB. A backup of the old report file is created. Up to three backups of old report files are saved. The oldest backups are deleted first.

## 11.7 Child Protection

Use Avira's *CHILD PROTECTION* features, to ensure a safe Internet experience for your children or other persons using your computer.

- With the **Social Networks** feature, you can monitor your children's activities online. The Social Networks technology checks their social network accounts for comments, photos etc. that may influence your child's reputation in a negative way or may indicate that your child is in danger.

**Related topics:**

- [Social Networks](#)

### 11.7.1 Social Networks

This chapter contains comprehensive information on

[Creating a Social Network Protection account](#)

[Logging in to your Social Network Protection account](#)

**Creating a Social Network Protection account**

- ▶ Make sure that your computer is connected to the internet.  
Click **Control Center > View > Child Protection > Social Networks**.  
Click **Get Started Now**.  
→ The web browser opens displaying the Avira Social Network Protection website.
- ▶ If you have a Facebook account, you can now log in to Avira Social Network Protection by clicking the **Facebook logo**.

-OR-

- ▶ If you do not have a Facebook account, enter your first name, your last name, your email address and a password in the required fields and click **Get Started**.

**Note**

From now on your email address will serve as your username.

**Logging in to an existing Social Network Protection account**

- ▶ Make sure that your computer is connected to the internet.
- ▶ Click **Control Center > View > Child Protection > Social Networks**.  
Click **Log in**.  
→ If you have saved the cookie on your system, the web browser opens displaying your Avira Social Network Protection dashboard.

-OR-



- If your web browser does not accept cookies or removes them every time your web browser is closed, you can either log in by clicking on the **Facebook logo** or by entering your username and password.

## 11.8 Mobile Protection

Avira does not only protect your computer system from malware and viruses but also protects your smartphone, running with Android operating system, from loss and theft. Using Avira Android Security you can also block unwanted calls or SMS. Simply add phone numbers from call log, SMS log and your list of contacts to the blacklist, or create manually a contact you want to block.

You can find more information on our website:

<http://www.avira.com/android>

## 11.9 General

### 11.9.1 Threat categories

*Selection of extended threat categories*

Your Avira product protects you against computer viruses. In addition, you can scan according to the following extended threat categories.

- [Adware](#)
- [Adware/Spyware](#)
- [Applications](#)
- [Backdoor Clients](#)
- [Dialer](#)
- [Double Extension Files](#)
- [Fraudulent software](#)
- [Games](#)
- [Jokes](#)
- [Phishing](#)
- [Programs that violate the private domain](#)
- [Unusual runtime packers](#)

By clicking on the relevant box, the selected type is enabled (check mark set) or disabled (no check mark).

## Select all

If this option is enabled, all types are enabled.

## Default values

This button restores the predefined default values.

### Note

If a type is disabled, files recognized as being of the relevant program type are no longer indicated. No entry is made in the report file.

## 11.9.2 Advanced protection

### *ProActiv*

#### Enable ProActiv

If this option is enabled, programs on your system are monitored and checked for suspicious actions. You will receive a message if typical malware behavior is detected. You can block the program or select "**Ignore**" to continue to use the program. The monitoring process excludes: Programs classified as trusted, trusted and signed programs included by default in the permitted applications filter, and all programs which you have added to the application filter for permitted programs.

ProActiv protects you from new and unknown threats for which there are not yet any virus definitions or heuristics available. ProActiv technology is integrated into the Real-Time Protection component and observes and analyzes the program actions performed. The behavior of the program is checked against typical malware action patterns: Type of action and action sequences. If a program exhibits typical malware behavior, this is treated as a virus detection: You have the option of blocking the program or ignoring the notification and continuing to use the program. You can classify the program as trusted and add it to the application filter for permitted programs. You have the option of adding the program to the application filter for blocked programs using the **Always block** command.

The ProActiv component uses rule sets developed by the Avira Malware Research Center to identify suspicious behavior. The rule sets are supplied by Avira databases. ProActiv sends information on any suspicious programs to the Avira databases for logging. During Avira installation, you have the option of disabling data transmission to the Avira databases.

### Note

ProActiv technology is not yet available for 64 bit systems!

### *Protection Cloud*

## Enable Protection Cloud

Fingerprints of all suspicious files are sent to the Protection Cloud for dynamic online inspection. Executables are instantly identified as clean, infected or unknown.

The Protection Cloud serves as a central location to observe attempted cyber attacks throughout our user base. The files accessed by your computer are matched against the fingerprints of files stored in the cloud. As more scanning is done in the cloud, less processing power is required by the antivirus application.

A list of file locations frequently targeted by malware is generated when the **Quick system scan** job runs. The list includes running processes, programs that run at start-up and services. The fingerprint of each file is generated and sent to the Protection Cloud, which is then categorized as "clean" or "malware". Unknown program files are uploaded to the Protection Cloud for analysis.

## Confirm manually when sending suspicious files to Avira

You can see a list of the suspicious files that should be sent to the Protection Cloud, and you can choose which files you want to send.

## Real-time file scanning

If this option is enabled, unknown files are sent to the Protection Cloud for analysis as soon as they are accessed.

## Show progress for uploads to the Avira Protection Cloud

A window displays the following information about the uploaded file(s) in form of a progress bar:

- file location
- file name
- status (uploading/analyzing)
- result (clean/infected)

## Blocked applications

Under *Applications to be blocked* you can enter applications which you classify as harmful and which you want Avira ProActiv to block by default. The applications added cannot be executed on your computer system. You can also add programs to the application filter for blocking via Real-Time Protection notifications of suspicious program behavior, by selecting the **Always block this program** option.

### *Applications to be blocked*

## Application

The list contains all applications which you have classified as harmful which you have entered via the configuration or by notifying the ProActiv component. The applications

on the list are blocked by Avira ProActiv and cannot be executed on your computer system. An operating system message appears when a blocked program starts up. The applications to be blocked are identified by Avira ProActiv on the basis of the path specified and the file name, and are blocked irrespective of their content.

### Input box

Enter the application you want to block in this box. To identify the application, the full path, file name and file extension must be specified. The path must either show the drive on which the application is located or start with an environment variable.



The button opens a window in which you can select the application to be blocked.

### Add

With the "**Add**" button you can transfer the application specified in the input box to the list of applications to be blocked.

#### Note

Applications required for the proper operation of the operating system cannot be added.

### Delete

The "**Delete**" button lets you remove a highlighted application from the list of applications to be blocked.

### Allowed applications

The section *Applications to be skipped* lists the applications excluded from monitoring by the ProActiv component: signed programs classified as trusted and included in list by default, all applications classified as trusted and added to the application filter: You can add permitted applications to the list in Configuration. You also have the option of adding applications to suspicious program behavior via Real-Time Protection notifications by using the **Trusted program** option in the Real-Time Protection notification.

#### *Applications to be skipped*

### Application

The list contains applications excluded from monitoring by the ProActiv component. In the default installation settings, the list contains signed applications from trusted vendors. You have the option of adding applications that you consider to be trustworthy via the configuration or via Real-Time Protection notifications. The ProActiv component identifies applications using the path, the file name and the content. We recommend checking the content as malware can be added to a program through changes such as updates. You can determine whether a contents check should be performed from the **Type** specified: For the "*Contents*" type, the applications specified

by path and file name are checked for changes to the file content before they are excluded from monitoring by the ProActiv component. If the file contents have been modified, the application is again monitored by the ProActiv component. For the "*Path*" type, no contents check is performed before the application is excluded from monitoring by the Real-Time Protection. To change the exclusion type, click on the type displayed.

**Warning**

Only use the *Path* type in exceptional cases. Malcode can be added to an application through an update. The originally harmless application is now malware.

**Note**

Some trusted applications, including for example all application components of your Avira product, are by default excluded from monitoring by the ProActiv component even though they are not included in the list.

**Input box**

In this box you enter the application to be excluded from monitoring by the ProActiv component. To identify the application, the full path, file name and file extension must be specified. The path must either show the drive on which the application is located or start with an environment variable.



The button opens a window in which you can select the application to be excluded.

**Add**

With the "**Add**" button you can transfer the application specified in the input box to the list of applications to be excluded.

**Delete**

The "**Delete**" button lets you remove a highlighted application from the list of applications to be excluded.

### 11.9.3 Password

You can protect your Avira product in [different areas](#) with a password. If a password has been issued, you will be asked for this password every time you want to open the protected area.

**Password**

## Enter password

Enter your required password here. For security reasons, the actual characters you type in this space are replaced by asterisks (\*). The password can only have a maximum of 20 chars. Once the password has been issued, the program refuses access if an incorrect password is entered. An empty box means "No password".

## Confirmation

Confirm the password entered above by entering again here. For security reasons, the actual characters you type in this space are replaced by asterisks (\*).

### Note

The password is case-sensitive!

## *Areas protected by password*

Your Avira product can protect individual areas with a password. By clicking the relevant box, the password request can be disabled or re-enabled for individual areas as required.

Password-protected area	Function
<b>Control Center</b>	If this option is enabled, the pre-defined password is required to start the Control Center.
<b>Activate / deactivate Real-Time Protection</b>	If this option is enabled, the pre-defined password is required to enable or disable Avira Real-Time Protection.
<b>Activate / deactivate Mail Protection</b>	If this option is enabled, the pre-defined password is required to enable/disable Mail Protection.
<b>Activate / deactivate Web Protection</b>	If this option is enabled, the pre-defined password is required to enable/disable Web Protection.

<b>Quarantine</b>	If this option is enabled, all areas of the quarantine manager protected by a password are enabled. By clicking on the relevant box, the password enquiry can be disabled or enabled again on request for individual areas.
<b>Restore affected objects</b>	If this option is enabled, the pre-defined password is required to restore an object.
<b>Rescan affected objects</b>	If this option is enabled, the pre-defined password is required to rescan an object.
<b>Affected object properties</b>	If this option is enabled, the pre-defined password is required to display the properties of an object.
<b>Delete affected objects</b>	If this option is enabled, the pre-defined password is required to delete an object.
<b>Send email to Avira</b>	If this option is enabled, the pre-defined password is required to send an object to the Avira Malware Research Center for examination.
<b>Configuration</b>	If this option is enabled, configuration of the program is only possible after entering the pre-defined password.
<b>Installation / uninstallation</b>	If this option is enabled, the pre-defined password is required for installation or uninstallation of the program.

## 11.9.4 Security

### *Autorun*

#### **Block autorun function**

If this option is enabled, the execution of the Windows autorun function is blocked on all connected drives, including USB sticks, CD and DVD drives and network drives. With the Windows autorun function, files on data media or network drives are read

immediately on loading or connection, and files can therefore be started and copied automatically. This functionality carries with it a high security risk, however, as malware and unwanted programs can be installed with the automatic start. The autorun function is especially critical for USB sticks as data on a stick can be changed at any time.

### **Exclude CDs and DVDs**

When this option is enabled, the autorun function is permitted on CD and DVD drives.

#### **Warning**

Only disable the autorun function for CD and DVD drives if you are sure you are only using trusted data media.

## *System protection*

### **Protect Windows hosts files from changes**

If this option is set to activated, the Windows hosts files are write-protected. Manipulation is no longer possible. For example, malware is not able to redirect you to undesired websites. This option is activated as the default setting.

## *Product protection*

#### **Note**

The product protection options are not available if the Real-Time Protection has not been installed using the user-defined installation option.

### **Protect processes from unwanted termination**

If this option is enabled, all processes of the program are protected against unwanted termination by viruses and malware or against 'uncontrolled' termination by a user, e.g. via Task-Manager. This option is enabled as the default setting.

#### **Advanced process protection**

If this option is enabled, all processes of the program are protected with advanced options against unwanted termination. Advanced process protection requires considerably more computer resources than simple process protection. The option is enabled as the default setting. To disable this option, you have to restart your computer.

#### **Note**

Process protection is not available for Windows XP 64 bit !



**Warning**

If process protection is enabled, interaction problems can occur with other software products. Disable process protection in these cases.

**Protect files and registry entries from manipulation**

If this option is enabled, all registry entries of the program and all program files (binary and configuration files) are protected from manipulation. Protection against manipulation entails preventing write, delete and, in some cases, read access to the registry entries or program files by users or external programs. To enable this option, you have to restart your computer.

**Warning**

Please note that, if this option is disabled, the repair of computers infected with specific types of malware may fail.

**Note**

When this option is activated, changes can only be made to the configuration, including changes to scan or update requests, by means of the user interface.

**Note**

Protection for files and registration entries is not available for Windows XP 64 bit !

## 11.9.5 WMI

### *Support for Windows Management Instrumentation*

Windows Management Instrumentation is a basic Windows management technology that uses script and programming languages to allow read and write access, both local and remote, to settings on Windows systems. Your Avira product supports WMI and provides data (status information, statistical data, reports, planned requests, etc.) as well as events via an interface. WMI gives you the option of downloading operating data from the program

**Enable WMI support**

When this option is enabled, you can download operating data from the program via WMI.

## 11.9.6 Events

### *Limit size of event database*

#### **Limit size to max. n entries**

If this option is enabled, the maximum number of events listed in the event database can be limited to a certain size; possible values: 100 to 10000 entries. If the number of entered entries is exceeded, the oldest entries are deleted.

#### **Delete all events older than n day(s)**

If this option is enabled, events listed in the event database are deleted after a certain period of time; possible values: 1 to 90 days. This option is enabled as the default setting, with a value of 30 days.

#### **No limit**

When this option has been activated, the size of the event database is not limited. However, a maximum of 20,000 entries are displayed in the program interface under Events.

## 11.9.7 Reports

### *Limit reports*

#### **Limit number to max. n piece**

When this option is enabled, the maximum number of reports can be limited to a specific amount. Values between 1 and 300 are permissible. If the specified number is exceeded, then the oldest report at that time is deleted.

#### **Delete all reports older than n day(s)**

If this option is enabled, reports are automatically deleted after a specific number of days. Permissible values are: 1 to 90 days. This option is enabled as the default setting, with a value of 30 days.

#### **No limit**

If this option is enabled, the number of reports is not restricted.

## 11.9.8 Directories

### *Temporary path*

#### **Use default system settings**

If this option is enabled, the settings of the system are used for handling temporary files.

#### Note

You can see where your system saves temporary files - for example with Windows XP - under: **Start > Settings > Control Panel > System > Index card "Advanced"** Button **"Environment Variables"**. The temporary variables (TEMP, TMP) for the currently registered user and for system variables (TEMP, TMP) are shown here with their relevant values.

### Use following directory

If this option is enabled, the path displayed in the input box is used.

#### Input box

In this input box, enter the path where the program will store its temporary files.



The button opens a window in which you can select the required temporary path.

#### Default

The button restores the pre-defined directory for the temporary path.

### 11.9.9 Acoustic alerts

When a virus or malware is detected by the System Scanner or Real-Time Protection, an acoustic alert is heard in interactive action mode. You can now choose to activate or deactivate the acoustic alert and select an alternative WAVE file for the alert.

#### Note

The action mode of the System Scanner is set in the configuration under [System Scanner > Scan > Action on detection](#). The action mode of the Real-Time Protection is set in the configuration under [Real-Time Protection > Scan > Action on detection](#).

### No warning

When this option is enabled, there is no acoustic alert when a virus is detected by the System Scanner or Real-Time Protection.

### Use PC speakers (only in interactive mode)

If this option is enabled, there is an acoustic alert with the default signal when a virus is detected by the System Scanner or Real-Time Protection. The acoustic alert is sounded on the PC's internal speaker.

**Use the following WAVE file (only in interactive mode)**

If this option is enabled, there is an acoustic alert with the selected WAVE file when a virus is detected by the System Scanner or Real-Time Protection. The selected WAVE file is played over a connected external speaker.

**WAVE file**

In this input box you can enter the name and the associated path of an audio file of your choice. The program's default acoustic signal is entered as standard.



The button opens a window in which you can select the required file with the aid of the file explorer.

**Test**

This button is used to test the selected WAVE file.

### 11.9.10 Alerts

Your Avira product generates so-called slide-ups, desktop notifications for specific events, which give information on successful or failed program sequences such as updates. Under **Alerts** you can enable or disable the notifications for specific events.

With desktop notifications, you have the option of disabling the notification directly in the slide-up. You can reactivate the notification, in the **Alerts** configuration window.

*Update***Alert, if last update is older than n day(s)**

In this box, you can enter the maximum number of days allowed to have passed since the last update. If this number of days has passed, a red icon is displayed for the update status under **Status** in the Control Center.

**Show notice if the virus definition file is out of date**

If this option is enabled, you will obtain an alert if the virus definition file is not up-to-date. With the help of the alert option, you can configure the temporal interval for an alert if the last update is older than n day(s).

*Warnings / Notes with the following situations***Dial-up connection is used**

If this option is enabled, you will receive a desktop notification alert if a dialer creates a dial-up connection on your computer via the telephone or ISDN network. There is a danger that the connection may have been created by an unknown and unwanted dialer and that the connection may be chargeable (see [Viruses and more > Threat categories: Dialer](#)).

**Files have been successfully updated**

If this option is enabled, you will receive a desktop notification whenever an update has been successfully performed and files updated.

**Update failed**

If this option is enabled, you will receive a desktop notification whenever an update fails: No connection to the download server could be created or the update files could not be installed.

**No update necessary**

If this option is enabled, you will receive a desktop notification whenever an update is started but installation of the files is not necessary as your program is up to date.



# Avira

This manual was created with great care. However, errors in design and contents cannot be excluded. The reproduction of this publication or parts thereof in any form is prohibited without previous written consent from Avira Operations GmbH & Co. KG.

Brand and product names are trademarks or registered trademarks of their respective owners. Protected trademarks are not marked as such in this manual. However, this does not mean that they may be used freely.

Issued Q4-2013

© 2013 Avira Operations GmbH & Co. KG. All rights reserved.  
Subject to change. Errors and omissions excepted.

Avira | Kaplaneiweg 1 | 88069 Tettnang | Germany | Telephone: +49 7542-500 0  
[www.avira.com](http://www.avira.com)